

IA agentique en banque et assurance

De l'expérimentation contrôlée à l'industrialisation maîtrisée

CGI

Finance Innovation

Sommaire

Synthèse exécutive p.6

Méthodologie et prise en main p.8

Introduction p.9

Pourquoi l'IA agentique impose un nouveau contrat de confiance

Acte 1 p.11

Où en sont réellement les banques et assurances face à l'IA agentique ?

Acte 2 p.18

Où l'IA agentique crée-t-elle réellement de la valeur ?

Acte 3 p.29

Comment industrialiser l'IA agentique dans un cadre maîtrisé ?

Acte 4 p.44

Quelle conduite du changement et quelle feuille de route ?

Conclusion générale p.54

De la puissance à la confiance

Expertise p.56

Remerciements p.60

Annexes p.61

Édito



Georges Harb

Vice-Président Senior en charge de l'intelligence artificielle pour CGI en France

L'intelligence artificielle entre dans une nouvelle phase de son développement. Après avoir démontré sa capacité à générer du contenu, assister les collaborateurs et accélérer l'accès à l'information, elle évolue désormais vers des systèmes capables d'orchestrer des actions, de coordonner des processus et d'interagir avec leur environnement : l'IA agentique, basée sur des agents (services) autonomes, communicants, performants mais surtout cadrés par l'humain.

Cette évolution ouvre des perspectives considérables pour les acteurs de la banque et de l'assurance. Les agents IA promettent d'améliorer l'expérience client, de renforcer les dispositifs de contrôle, d'accélérer les opérations et de valoriser plus efficacement le patrimoine informationnel des organisations. Toutefois, cette nouvelle étape soulève également des questions fondamentales. Lorsque l'IA ne se limite plus à produire une recommandation mais participe à l'exécution d'un processus, les enjeux de gouvernance, de supervision, de responsabilité et de confiance changent de dimension.

Les institutions financières disposent d'atouts importants pour relever ce défi. Elles ont développé au fil des années une culture exigeante de la gestion des risques, du contrôle et de la conformité. Mais elles doivent aujourd'hui trouver le bon équilibre entre l'innovation nécessaire pour rester compétitives et le niveau d'exigence attendu dans des environnements hautement réglementés.

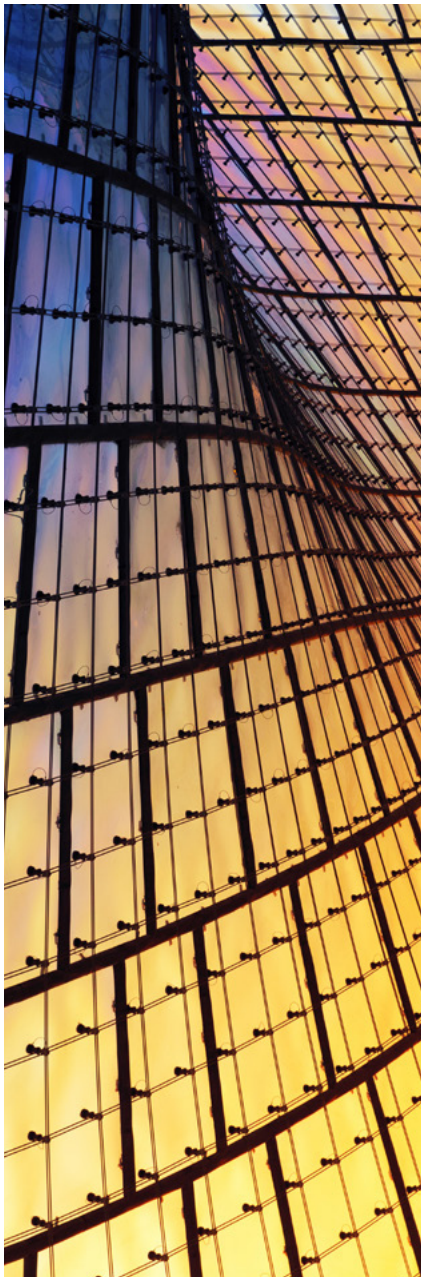
Les travaux menés avec Finance Innovation et les acteurs du secteur montrent une conviction largement partagée : le principal défi n'est plus d'identifier des cas d'usage. Les opportunités sont nombreuses et déjà bien identifiées. Le véritable enjeu réside désormais dans la capacité à industrialiser ces usages dans un cadre maîtrisé, en garantissant la qualité des données, la supervision humaine, l'explicabilité des décisions et la résilience des dispositifs mis en œuvre.

Chez CGI, nous sommes convaincus que l'avenir de l'IA agentique ne se construira pas autour d'une autonomie sans limite, mais autour d'une autonomie encadrée. La performance des agents devra s'accompagner de mécanismes robustes de contrôle, de traçabilité et de responsabilité. La confiance ne sera pas un bénéfice secondaire de l'agentique ; elle en sera la condition de réussite.

C'est précisément l'ambition de ce livre blanc. À travers les retours d'expérience, les enseignements issus des ateliers et les regards croisés d'experts du secteur, nous proposons d'explorer les conditions permettant de passer de l'expérimentation à l'industrialisation maîtrisée. Car dans les services financiers, la question n'est pas seulement de savoir ce que les agents IA pourront faire demain, mais dans quelles conditions les organisations pourront leur faire confiance.

La réussite de l'IA agentique ne reposera pas uniquement sur sa puissance technologique. Elle dépendra avant tout de notre capacité collective à construire un cadre de confiance durable et guidé par l'intelligence humaine, au service des collaborateurs, des clients et de la performance des organisations.

Édito





Dimitry Debenay

Directeur général de
Finance Innovation

L'IA agentique : augmenter l'humain, maîtriser la technologie

Après avoir exploré, en 2024 et en 2025, le potentiel de l'IA générative, nous abordons une étape nouvelle. Avec l'IA générative, nos organisations ont appris à interroger, résumer, produire et assister. Avec l'IA agentique, elles envisagent des systèmes qui reçoivent un objectif, décomposent une tâche, mobilisent des outils, enchaînent des étapes et, dans certains cas, agissent directement dans un processus métier.

La nuance paraît technique. Elle est stratégique. Tant qu'une IA produit un contenu, le contrôle porte sur la qualité d'une réponse. Dès qu'un agent prépare une décision ou déclenche une action, le contrôle porte sur l'ensemble du processus qui y conduit. Une erreur de génération devient une erreur d'exécution.

Dans la banque et l'assurance, cette bascule ne peut donc pas être traitée comme un simple gain de productivité. Nos métiers opèrent sous contrainte de conformité, de protection de la clientèle, de traçabilité et de responsabilité. La question n'est plus de savoir si un agent peut fonctionner : elle est de savoir à quelles conditions il peut être laissé en fonctionnement.

Les travaux menés avec CGI et un panel d'acteurs du secteur dessinent une position nette. Les professionnels ne rejettent pas l'IA agentique ; ils en reconnaissent la valeur. Mais ils refusent de confondre potentiel technologique et délégation de responsabilité. Ils attendent des agents qui préparent, sécurisent, accélèrent et augmentent, plutôt que des agents qui remplacent.

Trois enseignements méritent l'attention des dirigeants.

1 **La valeur immédiate, c'est le temps.**

Réduire les délais, absorber davantage de volume, améliorer la qualité de service. Le front office, la relation client et la distribution constituent le premier terrain d'adoption : ils concentrent les volumes, les informations à rassembler et l'exigence de réactivité.

2 **Le point de bascule n'est pas le cas d'usage, c'est l'industrialisation.**

Le problème n'est pas de manquer d'idées, mais de transformer des prototypes en solutions exploitables, contrôlées, auditées et économiquement soutenables. Le POC agentique est trompeur : il démontre la faisabilité technique avant d'exposer le coût complet — run, supervision humaine, tests continus, qualité des données, observabilité, sécurité et maintenance.

3 **La gouvernance est le principal facteur limitant.**

Elle n'est pas un frein à l'innovation : elle en est la condition. Une autonomie graduée, réversible, mesurable et explicable est ce qui permet d'avancer vite sans avancer à l'aveugle.

Deux convictions guident notre lecture.

L'innovation ne doit jamais réduire l'humain à un simple exécutant. Elle doit le libérer des tâches répétitives pour qu'il se concentre sur ce qui exige jugement, créativité et responsabilité. Avec une vigilance : le temps gagné sur l'exécution se déplace en partie vers la supervision. Superviser un agent est un savoir-faire nouveau, qui s'apprend, s'outille et s'organise.

La maîtrise technologique suppose un écosystème d'innovation souverain et résilient. Dépendre entièrement de solutions externes, c'est renoncer à une part de sa capacité d'adaptation et de décision. Nos laboratoires, nos start-up et nos entreprises ont les atouts pour construire une IA agentique responsable, ancrée dans les exigences propres à nos industries.

Nous remercions CGI pour la qualité de sa contribution, ainsi que l'ensemble des experts et des membres qui ont nourri ces travaux.

Ce livre blanc ne promet rien : il propose une méthode. Sélectionner les bons cas d'usage, industrialiser avec rigueur, gouverner dans la durée et accompagner celles et ceux qui feront vivre ces dispositifs.

C'est précisément le rôle de Finance Innovation : réunir les institutions financières, les start-ups, les chercheurs et les régulateurs pour que ces sujets soient traités ensemble, tôt, et sans naïveté.

Nos secteurs n'ont pas besoin d'une IA agentique spectaculaire. Ils ont besoin d'une IA agentique gouvernable. Elle n'en est qu'à ses débuts : à nous de la façonner selon nos valeurs.

Synthèse exécutive

L'IA agentique marque un changement de nature dans l'histoire récente de l'intelligence artificielle appliquée aux services financiers et assurantiels. Avec l'IA générative, les organisations ont appris à interroger, résumer, produire et assister. Avec l'agentique, elles envisagent désormais des systèmes capables de planifier une séquence d'actions, d'utiliser des outils, d'interagir avec plusieurs sources d'information, de contrôler des étapes et, dans certains cas, d'agir dans un workflow métier. Le système multi-agent vise à optimiser, valider et, dans certains cas, prendre lui-même des décisions. Ce déplacement est majeur : le risque ne porte plus seulement sur la qualité d'une réponse, mais **sur la qualité d'une action exécutée ou préparée par un système intelligent**.

Les ateliers et échanges révèlent une posture très nette. Les participants ne rejettent pas l'IA agentique ; au contraire, ils reconnaissent sa valeur. Mais ils refusent de confondre potentiel technologique et délégation de responsabilité. La maturité observée peut être qualifiée de prudente, mais constructive : les organisations veulent expérimenter, mais elles conditionnent le passage à l'échelle à des prérequis robustes de gouvernance, de supervision humaine, de qualité des données, d'explicabilité et d'acculturation.

Les participants perçoivent les agents comme des accélérateurs opérationnels : préparer, préanalyser, synthétiser, contrôler, orienter, recommander, remplir et sécuriser. Le premier terrain d'adoption ressort autour du front office, de la relation client et de la distribution, non parce que ces domaines seraient sans risque, mais parce qu'ils concentrent des volumes importants, des informations nombreuses, des tâches répétitives et une forte attente de réactivité. Le bénéfice dominant est



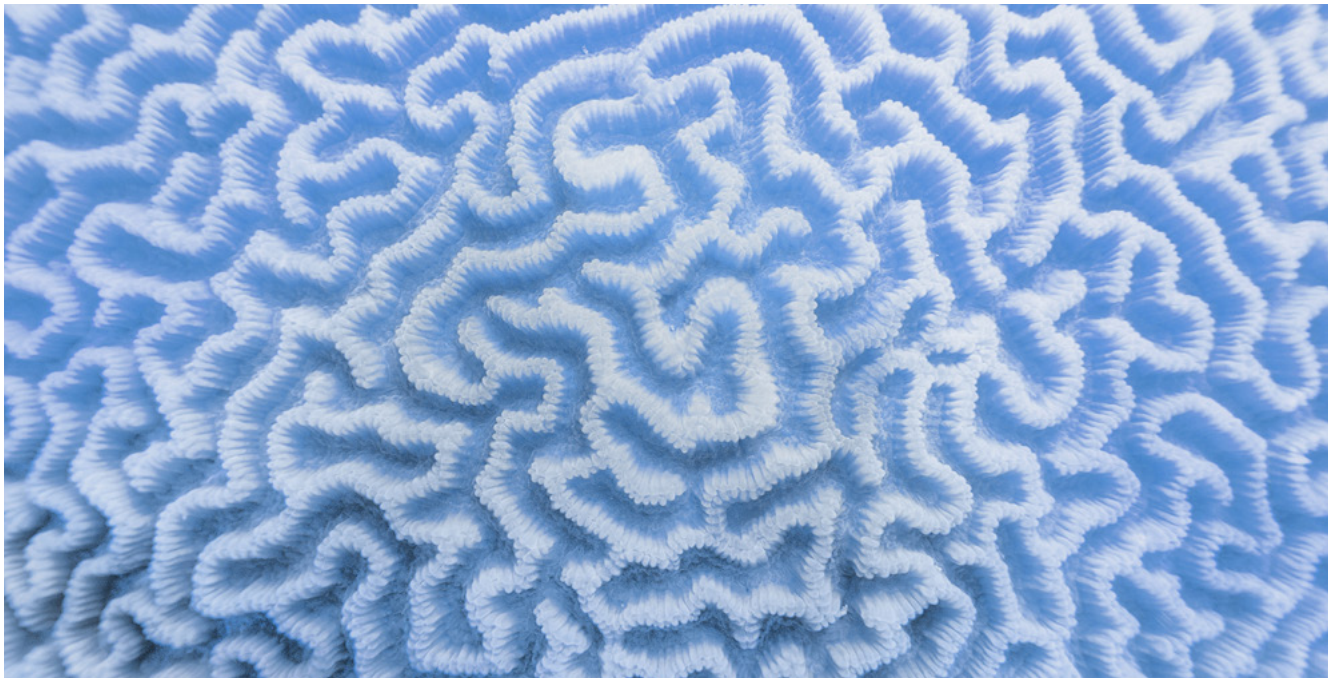
le temps : réduire les délais, augmenter la capacité de traitement, améliorer la qualité de service et absorber davantage de volume.

L'industrialisation constitue le vrai point de bascule. Les ateliers convergent vers une conviction structurante : le problème n'est pas le manque de cas d'usage, mais la capacité à les transformer en solutions exploitables, contrôlées, auditées et économiquement soutenables. Le POC agentique reste trompeur parce qu'il montre la faisabilité technique avant d'exposer le coût complet : run, tokens, supervision humaine, tests continus, qualité des données, observabilité, gestion des incidents, maintenance des prompts et des skills, gouvernance des modèles, sécurité, décommissionnement et responsabilité opérationnelle.

La vision 2030 exprimée dans les ateliers n'est pas celle d'une IA toute-puissante. Les participants attendent une IA capable de comprendre, anticiper, expliquer, représenter l'utilisateur et respecter les règles nativement. Mais ils posent des lignes rouges : pas de manipulation, pas d'influence invisible, pas de perte de libre arbitre, pas de décision sensible sans supervision humaine, pas d'agent non explicable ou non traçable. Le message de fond est donc clair : la puissance ne suffira pas ; la confiance deviendra la vraie infrastructure de l'agentique.

Le livre blanc présente une démarche de transformation structurée en quatre étapes. La première étape évalue le niveau de maturité de l'organisation et définit les prérequis à l'instauration d'un climat de confiance. La deuxième identifie les principaux leviers de création de valeur ainsi que les limites à ne pas franchir. La troisième expose une méthode d'industrialisation accompagnée d'un modèle de gouvernance adapté. Enfin, la quatrième est consacrée à la conduite du changement.

Ce dernier acte revêt une importance déterminante. Une organisation peut en effet disposer d'agents d'IA hautement performants et néanmoins échouer si les métiers, les managers, les fonctions de gestion des risques et les utilisateurs ne sont pas en mesure de les piloter, d'en interpréter les résultats, d'en remettre les décisions en question lorsque cela est nécessaire et de les faire évoluer dans la durée.



Méthodologie et prise en main

Méthodologie

Les réflexions et analyses présentées dans ce livre blanc résultent d'un travail collaboratif mené par Finance Innovation et CGI, accompagnés d'un panel d'acteurs de la banque et de l'assurance.

Notre démarche s'est appuyée sur deux ateliers :

- Un premier atelier début juin 2026 a réuni experts et contributeurs pour identifier les usages concrets de l'IA agentique dans la banque et l'assurance, croiser les regards, partager des retours d'expérience et mieux appréhender les limites actuelles ainsi que les premiers enjeux de gouvernance.
- Un second atelier fin juin 2026 a permis de faire émerger des orientations concrètes et structurantes pour maîtriser le passage à l'échelle dans un contexte sécurisé : modèles de gouvernance, architectures adaptées au passage à l'échelle, enjeux de performance, de coûts et de robustesse, exigences de sécurité, de conformité et de supervision.

Les synthèses et recommandations issues des ateliers ont ensuite été complétées par des interviews de membres du pôle Finance Innovation. Ce livre blanc synthétise l'ensemble de ces échanges, mettant en lumière les meilleures pratiques et les leviers clés pour une adoption réussie de l'IA agentique dans la banque et l'assurance.

Ce livre blanc est construit à partir d'une consolidation des résultats d'ateliers et d'un enrichissement documentaire externe. L'objectif n'est pas de produire une synthèse descriptive, mais un document exploitable par des décideurs banque, assurance, risques, conformité, métiers, IT et direction générale.

Par convention de lecture, lorsqu'aucune mention spécifique n'est indiquée, les analyses présentées dans ce document sont issues des échanges menés en ateliers, puis synthétisés et consolidés.

Certains passages sont signalés par une mention spécifique APPORT : ils correspondent à des éclairages, analyses ou mises en perspective complémentaires apportés par CGI.

Des références externes ont également été mobilisées pour compléter et mettre en perspective les travaux des ateliers, autour de quatre angles : conformité et régulation, gouvernance de l'IA, résilience opérationnelle et sécurité des applications agentiques.

Les principales références mobilisées sont : le règlement européen sur l'IA et ses lignes de classification, les travaux de l'EBA sur l'AI Act et l'adoption de l'IA dans le secteur bancaire, l'opinion de l'EIOPA sur la gouvernance de l'IA dans l'assurance, les publications de l'ACPR sur l'explicabilité et la gouvernance de l'IA en finance, DORA, les recommandations de la CNIL sur l'IA et le RGPD, le NIST AI RMF Generative AI Profile, la norme ISO/IEC 42001 et l'OWASP Agentic Top 10.

Les apports externes ne se substituent pas aux résultats des ateliers : ils les prolongent par un cadrage réglementaire, méthodologique ou opérationnel.

Introduction

Pourquoi l'IA agentique impose un nouveau contrat de confiance

Le terme d'IA agentique désigne une famille de systèmes capables d'aller au-delà de la génération d'une réponse. Un agent peut recevoir un objectif, décomposer une tâche, appeler des outils, consulter une base documentaire, interagir avec des systèmes, produire un résultat intermédiaire, s'autoévaluer, demander une validation humaine et poursuivre un workflow. Cette capacité d'action transforme le sujet : une erreur de génération devient potentiellement une erreur de processus.

Dans la banque et l'assurance, cette bascule intervient dans un environnement où l'acceptabilité ne dépend jamais de la performance seule. Le secteur opère sous contrainte de conformité, de protection de la clientèle, de secret, de solvabilité, de lutte contre la fraude, de lutte contre le blanchiment, de continuité d'activité, de traçabilité, de contrôle interne et de responsabilité. L'agentique ne peut donc pas être abordée comme un simple empilement d'outils de productivité.

Les résultats d'atelier confirment cette spécificité. Les participants savent identifier des cas d'usage concrets, mais ils posent spontanément la question du cadre : qui supervise, qui décide, qui valide, qui arrête, qui assume, qui audite, qui explique ? Le sujet n'est plus de savoir si un agent peut fonctionner ; il est de savoir dans quelles conditions il peut être laissé en fonctionnement.

Ce livre blanc propose donc une lecture volontairement opérationnelle. Il ne s'agit ni de promouvoir l'autonomie pour elle-même ni de figer l'organisation dans la prudence. La bonne trajectoire consiste à organiser une autonomie graduée, réversible, mesurée et gouvernée.

« À chaque type d'utilisation de l'IA quasi autonome doit correspondre une solution de maîtrise du risque. »

Florence Picard
Membre agrégé de l'Institut des Actuaires

Ce que promet le marché, ce que demandent les organisations

Le marché met en avant l'image de l'employé numérique autonome : disponible en permanence, capable d'enchaîner des actions, de répondre aux clients, de gérer des exceptions et de réduire les coûts. Les participants ne demandent pas prioritairement un agent qui remplace un dispositif humain ; ils demandent un agent qui prépare, sécurise, accélère et augmente. La différence est décisive : le premier imaginaire repose sur la délégation ; le second repose sur la coopération.

Cette coopération ne sera pas neutre pour les organisations. Un agent qui prépare un rendez-vous modifie le rôle du conseiller. Un agent qui analyse des réclamations modifie le rôle du manager opérationnel. Un agent qui surveille la conformité modifie le rôle du contrôle permanent. Un agent qui rédige ou consolide un rapport réglementaire modifie la relation entre métier, conformité, data et IT.

La véritable valeur de l'IA agentique ne réside pas d'abord dans la manière dont l'utilisateur interagit avec elle, mais dans sa capacité à exécuter des tâches et à contribuer à l'orchestration de processus complexes de manière autonome.

> « Le terme "agent IA" est devenu un mot-valise qui recouvre des systèmes très différents. Avant de parler d'adoption, il faut d'abord clarifier le niveau d'autonomie que l'on souhaite réellement accorder à l'agent. »

Jean-Michel Ghidaglia
Cofondateur, Deepika

L'IA agentique créera de la valeur dans les services financiers si elle est conçue comme une capacité à contribuer, de manière autonome et maîtrisée, à l'exécution et à l'orchestration des processus métier : utile aux métiers, contrainte par la qualité des données, supervisée par l'humain, explicable pour l'audit et gouvernée dans la durée.

Acte 1

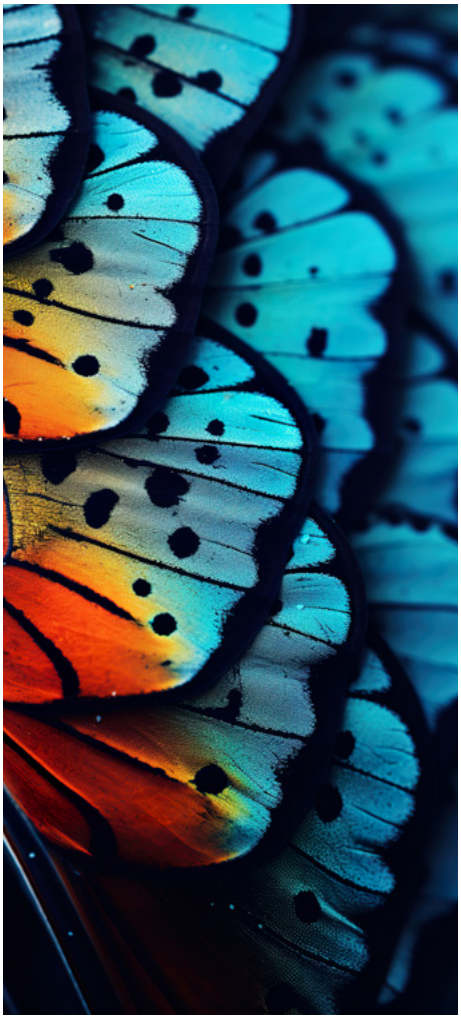
Où en sont réellement les banques et assurances face à l'IA agentique ?

Les organisations financières sont-elles prêtes à faire confiance à des agents capables d'agir ?

La réponse appelle une nuance. Les acteurs du secteur reconnaissent le potentiel de création de valeur de l'IA agentique, mais ils ne sont pas prêts à lui déléguer une autonomie significative sans un cadre de contrôle renforcé. La maturité observée ne traduit ni un enthousiasme aveugle ni une posture de rejet. Elle reflète un pragmatisme propre aux services financiers : expérimenter les capacités offertes par les agents, oui ; leur confier des décisions ou des actions sans gouvernance, supervision humaine et mécanismes d'audit, non.



1.1 Une maturité prudente, mais constructive



Les contributions de la première séquence convergent vers cinq prérequis de confiance : gouvernance, supervision humaine, qualité des données, explicabilité, transformation. Ces prérequis ne sont pas périphériques ; ils déterminent l'acceptabilité même de l'agentique. Dans un secteur où les décisions peuvent produire des effets financiers, juridiques ou sociaux, la valeur ne compense pas l'absence de contrôle.

La maturité se situe entre l'expérimentation et l'adoption contrôlée. Les acteurs ne rejettent pas l'autonomie, mais ils l'adossent à des paliers. L'agent peut préparer, assister, contrôler ou recommander. Il ne peut pas devenir souverain sur des décisions critiques sans supervision, auditabilité et responsabilité explicites.

APPORT

La maturité agentique peut être lue selon quatre niveaux. Le premier est l'exploration : les équipes testent des assistants et des prototypes. Le deuxième est l'expérimentation : les cas d'usage sont cadrés, mais restent hors production ou limités. Le troisième est l'adoption contrôlée : les agents sont intégrés à des workflows, avec validation humaine et supervision. Le quatrième est l'autonomie encadrée : l'agent agit sur un périmètre limité, observable, interruptible, réversible et auditable.

« Le principal frein à l'adoption de l'IA agentique, c'est de ne pas avoir compris qu'il s'agit d'abord d'une question de processus métier avant d'être une question d'automatisation. »

Ossama Benbouidda
Responsable processus et organisation, Groupe Caisse des Dépôts

1.2 La gouvernance comme facteur limitant principal

La gouvernance ressort comme le principal facteur limitant. Les participants évoquent un cadre de pilotage, des responsabilités définies, des règles métier communes, l'auditabilité et le contrôle continu. Cette récurrence indique que le sujet n'est plus seulement technologique. Les organisations savent qu'un agent peut fonctionner ; elles s'interrogent sur la manière de le piloter et de le gouverner lorsqu'il fonctionne.

APPORT

La gouvernance agentique doit combiner trois couches : la gouvernance stratégique, qui fixe les objectifs et les lignes rouges ; la gouvernance opérationnelle, qui encadre les droits, les rôles, les processus et les KPI ; la gouvernance technique, qui assure la sécurité, l'observabilité, les tests, la gestion des versions, le monitoring et le décommissionnement.



La référence ACPR sur la gouvernance de l'IA en finance renforce cette lecture : l'intégration d'un composant d'IA dans un processus métier influe sur sa gouvernance dès la conception, notamment lorsque la fonction est critique ou présente un risque de conformité. Le besoin de reproductibilité, d'auditabilité, de monitoring et d'explication n'est donc pas un luxe méthodologique, mais un principe de contrôle.

« Le sujet n'est déjà plus seulement de faire émerger des cas d'usage : il devient nécessaire de les prioriser, de mesurer leur valeur et d'organiser une véritable roadmap IA. »

Patrick Pansier

Responsable Data, Digital & Innovation, LBP AM

Vision opérationnelle

Des impacts sur la gouvernance

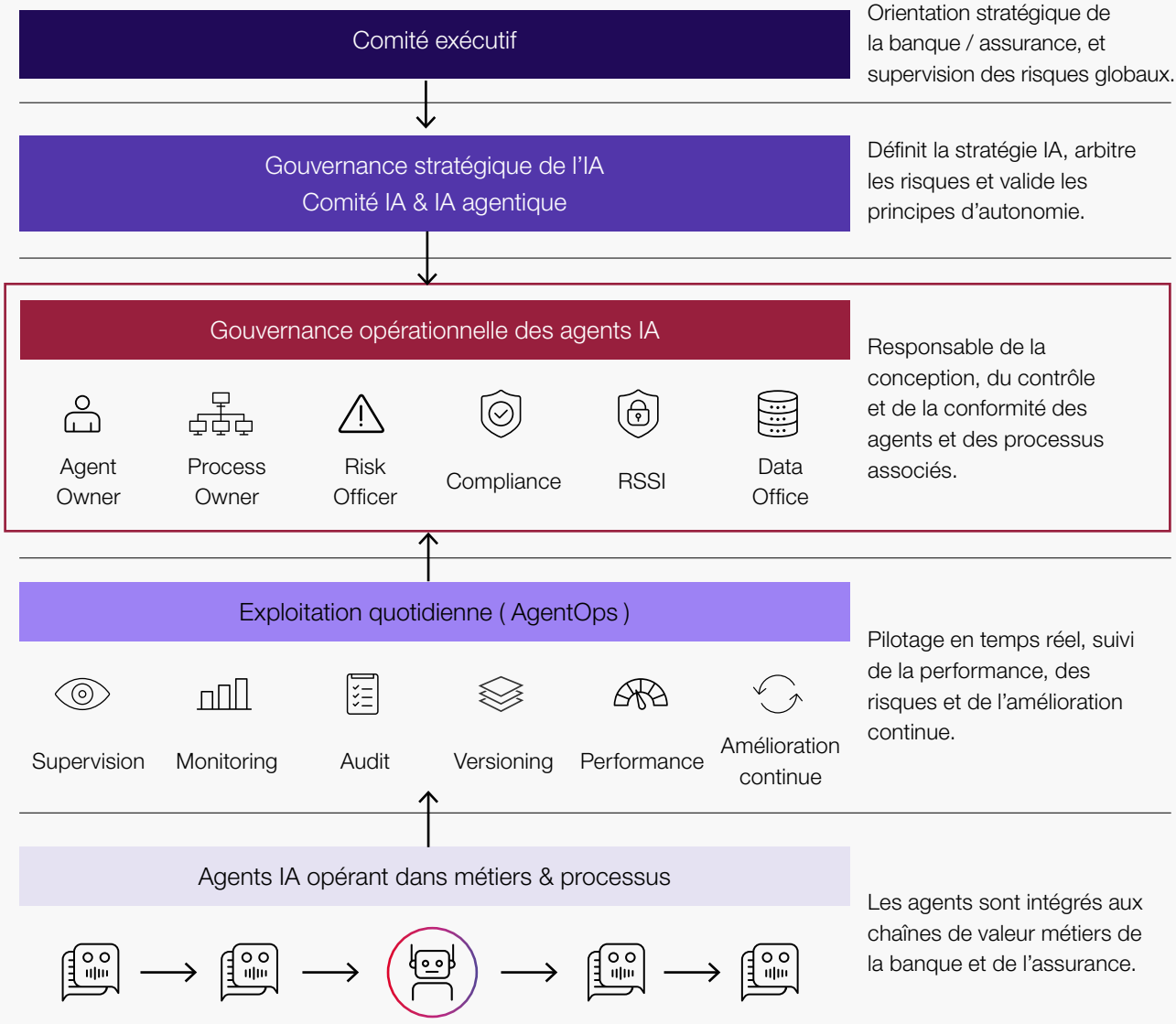
L'IA agentique introduit un nouvel objet de gouvernance : l'agent autonome.

Il devient nécessaire d'ajouter une couche de gouvernance spécifique.

Objectif

Piloter les agents IA comme des actifs métiers, avec un cycle de vie, un propriétaire et des mécanismes de supervision.

La nouvelle gouvernance



1.3 L'humain reste au centre, mais son rôle change

Les notions de supervision humaine, contrôle de résultat, validation des décisions sensibles et « Human-in-the-loop » reviennent fortement. Les agents sont perçus comme des copilotes avancés, pas comme des décideurs autonomes.

L'humain ne disparaît pas ; son rôle évolue. Il n'a plus vocation à exécuter systématiquement chaque tâche, mais à comprendre les raisonnements de l'agent, arbitrer les situations complexes, contrôler les résultats, remettre en question les décisions lorsque cela est nécessaire et en assumer la responsabilité. Cette évolution va bien au-delà du simple principe de « l'humain dans la boucle ». Un opérateur qui valide une décision sans en comprendre les fondements n'apporte qu'une garantie de façade. À l'inverse, un humain capable d'interroger, de contester et, si nécessaire, de corriger les propositions de l'agent constitue un véritable mécanisme de maîtrise des risques.

APPORT

La notion de « Human-in-the-loop » doit être précisée. Elle peut désigner une validation systématique, une validation par seuil de risque, un échantillonnage statistique, une supervision ex post, une escalade sur exception ou une possibilité de débrayage. Chaque cas d'usage doit expliciter le mode de supervision retenu, car les implications en matière de coût, de responsabilité et de valeur sont très différentes.

« La France est peut-être plus en retard parce que nous sommes très imprégnés de réglementation et de conformité, mais aussi parce qu'il existe une différence culturelle face au risque social : l'IA est associée à la perte d'emplois et à la déshumanisation. »

Florence Picard
Membre agrégé de l'Institut des Actuaires

1.4 La donnée comme socle de confiance

La qualité des données est identifiée comme le risque numéro un. Un agent amplifie ce qu'il consomme. Si les données sont incomplètes, contradictoires, non gouvernées ou obsolètes, il peut accélérer la diffusion d'erreurs au lieu de créer de la valeur.

APPORT

Pour l'agentique, la donnée ne doit pas être réduite à la donnée structurée. Elle inclut les documents, les règles métier, les historiques de décisions, les échanges clients, les procédures, les référentiels de conformité, les logs, les exceptions et les connaissances tacites rendues explicites. L'enjeu n'est donc pas seulement la qualité de la data ; c'est la qualité du contexte accessible à l'agent.



1.5 L'explicabilité devient un prérequis d'adoption

Les participants demandent que l'agent justifie ses sources, ses hypothèses, son niveau de confiance et les alternatives écartées. Ils expriment un besoin de comprendre pourquoi l'agent agit ou recommande.

L'explicabilité répond à trois attentes simultanées : conformité, audit et adoption. Le conseiller doit comprendre ce qu'il utilise ; le contrôleur doit pouvoir vérifier ; le client doit recevoir des explications notamment lorsque ses intérêts sont affectés. L'explicabilité ne se limite pas à une capacité technique ; elle constitue un levier essentiel de confiance, de gouvernance et de responsabilité.

APPORT

Il est pertinent de distinguer quatre niveaux d'explication, dans la continuité des travaux de l'ACPR : l'observation du résultat produit, la justification de la recommandation formulée, l'approximation du comportement du modèle et la réplication du processus de décision, permettant d'en rejouer les différentes étapes. Tous les cas d'usage ne requièrent pas le même niveau d'explication ; en revanche, chacun devrait définir explicitement le niveau d'explicabilité attendu en fonction des enjeux métiers, réglementaires et opérationnels.

1.6 L'acculturation : le facteur souvent sous-estimé

L'acculturation est considérée comme aussi importante que la technologie. Les participants mentionnent la pédagogie, la formation, le développement des compétences en IA et la conduite du changement. Le risque formulé est fort : disposer d'agents performants dans une organisation qui ne sait pas les utiliser.

APPORT

L'acculturation doit être différenciée. La direction générale a besoin de comprendre les arbitrages de valeur, de risque et de souveraineté. Les métiers doivent savoir qualifier les tâches et interpréter les recommandations. Les fonctions risques et conformité doivent savoir auditer les agents. L'IT doit savoir les exploiter, les monitorer et les sécuriser. Les managers doivent apprendre à piloter des équipes hybrides humains-agents.



Le paradoxe stratégique

Les participants perçoivent simultanément le risque de faire trop vite et le risque de ne pas aller assez vite. Ils demandent du contrôle, mais craignent le retard concurrentiel et l'adoption des agents par les clients avant les entreprises.

« Avec l'IA, on ne peut pas se contenter d'électrifier la bougie : il faut parfois changer complètement de paradigme et réimaginer le processus métier. »

Ossama Benbouidda
Responsable processus et organisation, Groupe Caisse des Dépôts

« Pour une petite structure comme la nôtre, l'IA n'est pas un frein : elle répond justement à un besoin de productivité que nous ne pourrions pas toujours couvrir par du recrutement. »

Guy-Matthieu Verwaerde
CEO et Cofondateur, StudyAssur

Acte 2

Où l'IA agentique crée-t-elle réellement de la valeur ?

Si les agents arrivent demain dans l'organisation, où seront-ils réellement utilisés ?

Les participants voient l'IA agentique comme un accélérateur opérationnel avant d'être un remplaçant de l'humain. Les cas d'usage relèvent majoritairement de la préparation, de la coordination, du contrôle, de l'assistance, de la synthèse et de l'automatisation de tâches répétitives.

Trois rôles émergents de l'agent dans les services financiers



Assistant opérationnel

- Préparation
- Pré-analyse
- Pré-remplissage
- Synthèse



Contrôleur permanent

- Audit de processus
- Conformité
- Surveillance
- Contrôle continu



Diffuseur de savoir

- Capitalisation
- Connaissances
- Meilleures pratiques
- Support dirigeants

2.1 Le gain dominant : le temps avant les coûts



Le bénéfice évoqué le plus souvent est le temps : raccourcir les délais, accélérer les traitements, augmenter la capacité de traitement, améliorer la réactivité. La réduction de coûts apparaît plus indirectement, souvent derrière l'idée de soulager les équipes.

Cette formulation est importante. Elle évite de réduire l'agentique à un projet de substitution. Les participants l'associent à une augmentation de capacité : traiter davantage de demandes, mieux préparer les décisions, réduire les oublis, fiabiliser l'exécution et améliorer la qualité de service.

APPORT

La valeur doit être mesurée par plusieurs métriques et non par le seul coût salarial évité puisque l'objectif n'est pas de réduire les effectifs. Elle doit être appréciée au moyen d'un ensemble d'indicateurs reflétant à la fois la performance opérationnelle, la qualité de service et la maîtrise des risques. Parmi ceux-ci figurent notamment le délai moyen de traitement, le taux de dossiers complets, le taux de réouverture, le taux d'erreur, la satisfaction des collaborateurs et des clients, le volume d'activité absorbé, la qualité des explications fournies, le niveau d'autonomie atteint sans incident, ainsi que les coûts de traitement et de supervision.

« La création de valeur est très concrète : automatiser les demandes simples permet de libérer du temps humain tout en offrant un service disponible 24 heures sur 24 et capable de traiter plusieurs clients simultanément. »

Guy-Matthieu Verwaerde
CEO et Cofondateur, StudyAssur

2.2 De l'optimisation des tâches à la transformation des chaînes de valeur

L'enjeu n'est plus de savoir si l'IA agentique peut automatiser certaines tâches, mais d'identifier où elle crée une valeur métier durable. Dans les secteurs de la banque et de l'assurance, la question n'est pas « Où déployer un agent IA ? », mais « Quels objectifs stratégiques souhaitons-nous atteindre, avec quel niveau d'autonomie et de maîtrise du risque ? ».

L'identification des cas d'usage ne peut se limiter à l'automatisation de tâches isolées. La création de valeur apparaît lorsque l'IA s'intègre aux chaînes de valeur de bout en bout — de l'acquisition client à la conformité, de la souscription à la gestion des sinistres ou des crédits — afin d'améliorer les processus, la qualité de service, la maîtrise des risques et la performance opérationnelle.



APPORT

Le choix d'un cas d'usage doit avant tout répondre à un objectif métier clair : améliorer l'expérience client, réduire les délais, renforcer la conformité, limiter les erreurs ou accroître la résilience de l'organisation. L'IA agentique n'est cependant pas une solution universelle ; selon les besoins, une automatisation classique, un moteur de règles ou un copilote peut s'avérer plus pertinent. La priorité est donc de sélectionner le niveau d'intelligence et d'autonomie le plus adapté au contexte.

« Si je devais lancer un seul cas d'usage agentique, je choisirais la conformité opérationnelle, car elle combine des règles déjà établies, des volumes importants et un fort potentiel de gains d'efficacité. »

Tang Loaec
Cofondateur, Deepika

De l’optimisation de tâches à la chaîne de valeur

Prioriser les cas d’usage IA selon la valeur métier, les risques et l’effort de mise en œuvre

OPTIMISATION DE TÂCHES → TRANSFORMATION DES CHAÎNES DE VALEUR

1 Définir les objectifs métier

- Expérience client
- Réduction des délais
- Conformité renforcée
- Productivité accrue
- Qualité opérationnelle
- Maîtrise des risques
- Résilience opérationnelle

2 Analyser le parcours complet

- Banque : Acquisition, KYC, Conseil, Crédit, Opérations, Relation client, Risques, Conformité, IT.
- Assurance : Acquisition, Devis, Souscription, Contrat, Sinistre, Indemnisation, Fraude, Reporting, IT.

3 Choisir la bonne réponse

- Automatisation classique
- Moteur de règles
- Algorithme simple
- IA prédictive traditionnelle
- IA générative
- Copilote métier
- Agent IA (plus autonome)

4 Prioriser selon l’équilibre recherché

- Valeur métier attendue
- Risque client, réglementaire, opérationnel et réputationnel
- Effort d’intégration et de mise en œuvre
- Qualité des données disponibles
- Supervision humaine et gouvernance
- Coût complet (TCO), déploiement et MCO

5 Focaliser les investissements

- Sélectionner les cas d’usage les plus alignés avec les objectifs stratégiques
- Privilégier les cas à fort impact, maîtrisables et plus rapidement industrialisables
- Créer de la valeur durable et mesurable à l’échelle

2.3 Cartographie des familles de cas d'usage

Les travaux de l'atelier ont mis en évidence que la valeur de l'IA agentique ne réside pas dans le remplacement d'une fonction, mais dans sa capacité à renforcer chaque étape de la chaîne de valeur des établissements financiers. Plutôt qu'un agent généraliste, les participants convergent vers une approche fondée sur **des agents spécialisés**, chacun étant conçu pour assister un métier, un processus ou une famille d'activités spécifiques.

« Tous les processus de back-office sont particulièrement éligibles à l'IA agentique : back-office bancaire, assurantiel, gestion de politiques publiques ou encore contrôles de premier niveau. »

Ossama Benbouidda
Responsable processus et organisation, Groupe Caisse des Dépôts

APPORT

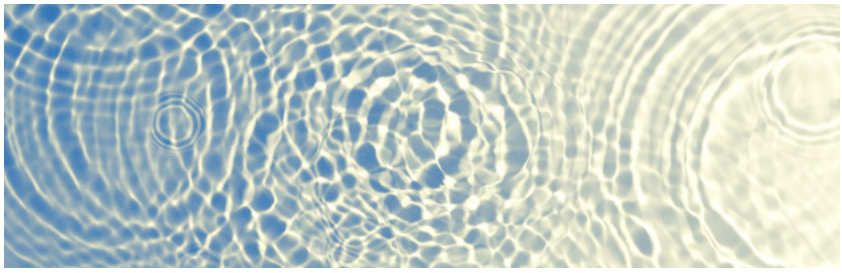
Cette cartographie propose une lecture des principaux cas d'usage selon les trois grands domaines opérationnels des organisations financières : le **Front Office**, où l'enjeu est d'améliorer la relation client et le développement commercial ; le **Middle Office**, centré sur la maîtrise des risques, de la conformité et des contrôles ; et le **Back Office**, dont la priorité est l'automatisation des traitements, la qualité opérationnelle et l'efficacité des processus.

Au sein de chacun de ces domaines, les agents IA interviennent principalement comme des **assistants opérationnels**. Ils préparent les dossiers, analysent les informations, vérifient les données, orchestrent les traitements, détectent les anomalies et proposent des recommandations aux collaborateurs. Cette répartition illustre un principe fort dégagé lors de l'atelier : **l'IA crée davantage de valeur lorsqu'elle augmente les capacités des experts métiers qu'elle ne cherche à se substituer à eux.**



La cartographie met également en évidence l'émergence d'un **nouveau modèle opérationnel**, dans lequel le collaborateur devient le chef d'orchestre d'un ensemble d'agents spécialisés. Ceux-ci prennent en charge les activités répétitives, les analyses préparatoires et les contrôles de premier niveau, tandis que les décisions engageantes, les arbitrages et la responsabilité finale demeurent sous supervision humaine.

Cette représentation n'a pas vocation à être exhaustive. Elle illustre une conviction partagée par les participants : **le déploiement de l'IA agentique ne transforme pas uniquement les outils, mais la manière dont les métiers collaborent, prennent leurs décisions et organisent leurs processus.**



« Pour les générations les plus jeunes, tout se gère déjà depuis un téléphone. L'IA agentique va accélérer une transformation de la relation client qui est en réalité déjà engagée. »

Guy-Matthieu Verwaerde
CEO et Cofondateur, StudyAssur

« Sur des processus comme les RFP, les NDA ou les commentaires de gestion, l'IA permet d'accélérer le traitement tout en s'appuyant sur le contexte et les données propres au métier. »

Patrick Pansier
Responsable Data Digital & Innovation, LBP AM

Le problème n'est pas le manque de cas d'usage. Les participants en identifient rapidement plusieurs dizaines. Le défi reste de les industrialiser dans un cadre maîtrisé : gouvernance, qualité des données, supervision et contrôle continu.

Cartographie des usages & valeur créée

Des agents IA spécialisés au service des métiers pour plus de valeur, de productivité et de conformité

FRONT OFFICE
Le conseiller augmenté

Renforcer la relation client, développer le business et améliorer l'expérience

PRINCIPAUX CAS D'USAGE

Agent Préparation, Rendez-vous

- Analyse 360° client et contexte
- Prépare un briefing complet et personnalisé

Agent Prospection

- Détecte et priorise les prospects
- Personnalise les messages et relance

Agent Recommandation

- Propose des solutions adaptées en temps réel
- Simule, évalue les risques et arguments

Agent Post-entretien & Suivi

- Rédige le compte rendu et met à jour le CRM
- Crée les tâches et assure le suivi commercial

MIDDLE OFFICE
L'analyste augmenté

Sécuriser, contrôler et piloter les processus à forte valeur réglementaire et de risque

PRINCIPAUX CAS D'USAGE

Agent KYC / Onboarding

- Collecte et vérifie les documents
- Prépare le dossier pour validation

Agent Conformité Réglementaire

- Analyse les nouvelles réglementations
- Identifie les impacts et propose les contrôles

Agent Risques & Surveillance

- Surveille les portefeuilles et détecte les anomalies
- Alerte et propose des scénarios de traitement

Agent AML / LBC-FT

- Enrichit et priorise les alertes
- Propose un niveau de risque et prépare l'investigation

Agent Réconciliation & Contrôles

- Rapproche les opérations et détecte les écarts
- Interroge les systèmes et propose une résolution

BACK OFFICE
L'opérateur augmenté

Automatiser à grande échelle les traitements pour gagner en efficacité et en qualité

PRINCIPAUX CAS D'USAGE

Agent Traitement dossier de crédit

- Récupère, vérifie et analyse les documents
- Produit une synthèse et prépare la décision

Agent Paiements

- Vérifie les flux et détecte les anomalies
- Déclenche les investigations et corrections

Agent Réclamations

- Comprend le contexte et recherche l'historique
- Rédige une réponse et transmet au collaborateur

Agent Gestion documentaire

- Classe et extrait les données
- Vérifie la cohérence et alimente les applications

NOUVEAU MODÈLE OPÉRATIONNEL

Le collaborateur devient chef d'orchestre, assisté par des agents IA spécialisés qui exécutent, analysent et préparent.

PRINCIPE DE FONCTIONNEMENT

- Orchestration et collaboration humain + IA
- Supervision humaine pour les décisions sensibles
- Traçabilité, audit et conformité intégrés



2.4 Risques versus valeur

Les travaux menés dans le cadre de l'atelier ont mis en évidence que tous les cas d'usage d'IA agentique ne présentent ni le même potentiel de création de valeur ni le même niveau de risque. Si certains agents interviennent principalement en assistance des collaborateurs — en préparant, synthétisant, contrôlant ou orchestrant des activités — d'autres se situent au plus près de décisions susceptibles d'avoir des conséquences pour le client, l'établissement ou le respect des exigences réglementaires. Ce constat conduit à considérer que la priorisation des cas d'usage doit reposer sur une évaluation croisée de la valeur métier attendue et du niveau de risque associé, afin d'orienter les investissements vers les usages offrant le meilleur équilibre entre impact, maîtrise des risques et faisabilité.

« Pour moi, le risque de fraude devient énorme. L'IA peut être très utile pour nous aider à maîtriser et à connaître ce risque qu'elle contribue par ailleurs à produire. »

Florence Picard
Membre agrégé de l'Institut des Actuaires

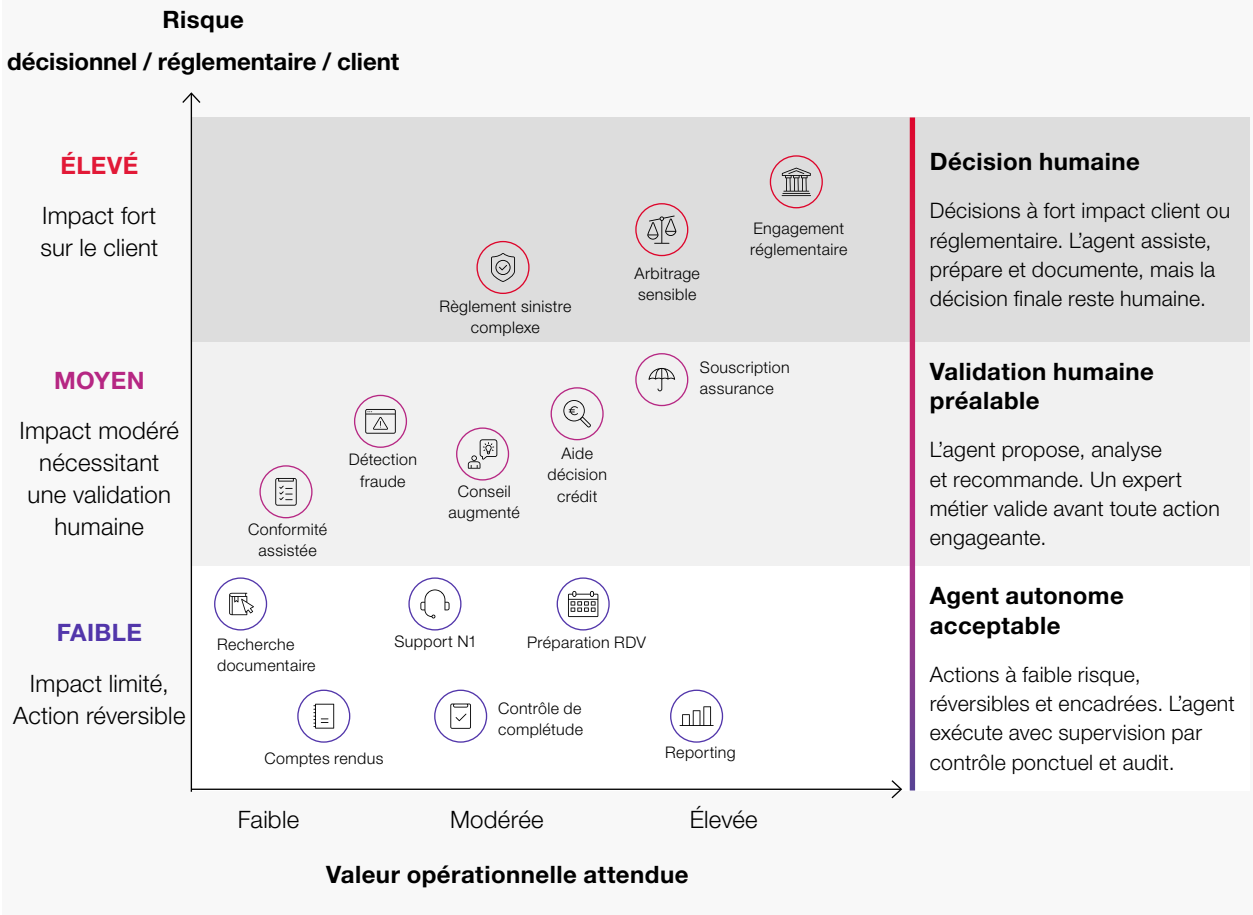
APPORT

La matrice valeur / risque constitue un outil d'aide à la décision permettant d'évaluer chaque cas d'usage selon deux dimensions complémentaires. La première concerne la valeur créée pour l'organisation : amélioration de la qualité de service, réduction des délais, gains de productivité, diminution des erreurs ou renforcement de la performance opérationnelle. La seconde porte sur le niveau de risque induit : impact potentiel d'une erreur, exposition du client, caractère réversible des actions, exigences de conformité, enjeux juridiques ou réputationnels et degré d'autonomie accordé à l'agent.

Cette approche est particulièrement pertinente dans les secteurs de la banque et de l'assurance, où les exigences de gouvernance et de maîtrise des risques sont élevées. Les usages impliquant des décisions susceptibles d'affecter les droits ou les intérêts des clients — par exemple l'évaluation de la solvabilité, le scoring de crédit ou certaines décisions de souscription — nécessitent un niveau de contrôle renforcé et relèvent, pour certains, des catégories de systèmes à haut risque définies par le cadre réglementaire européen.

L'objectif de cette matrice n'est pas de classer définitivement les cas d'usage, mais d'éclairer les choix d'investissement et de déploiement. Plus un agent IA se rapproche d'une décision engageante, plus les exigences en matière de supervision humaine, de traçabilité, d'explicabilité et d'auditabilité deviennent déterminantes. À l'inverse, les usages centrés sur la préparation, la vérification ou l'assistance opérationnelle offrent généralement un meilleur équilibre entre création de valeur, maîtrise des risques et facilité d'industrialisation.

Matrice valeur / risque des cas d'usage agentiques dans les services financiers



2.5 Les lignes rouges de l’IA agentique

Plusieurs principes de vigilance se dégagent et constituent autant de lignes rouges pour un déploiement responsable de l'IA agentique dans les secteurs de la banque et de l'assurance.

- **Ne pas déléguer à un agent IA une décision réglementairement ou juridiquement engageante sans validation humaine.** Les décisions produisant des effets sur les droits, les obligations ou la situation d'un client doivent rester sous la responsabilité d'un décideur humain.
- **Ne pas déployer un agent autonome en interaction avec les clients sans un dispositif de supervision adapté. Une information transparente, des mécanismes de monitoring,** des procédures d'escalade et une intervention humaine doivent pouvoir être mobilisés à tout moment.
- **Ne pas connecter un agent à des systèmes critiques sans gouvernance technique robuste. La gestion des habilitations, la journalisation des actions,** la séparation des tâches et la capacité de retour arrière (rollback) constituent des prérequis indispensables.
- **Ne pas assimiler un démonstrateur (POC) à une solution industrialisable.** La réussite d'une expérimentation ne garantit ni la robustesse, ni la sécurité, ni la conformité, ni l'auditabilité nécessaires à un déploiement en production.



- **Ne pas limiter l'évaluation de la valeur de l'IA agentique à la seule réduction des coûts ou des effectifs. Les bénéfices identifiés par les participants concernent en priorité les gains de temps,** l'augmentation des capacités de traitement, l'amélioration de la qualité de service et le renforcement de la maîtrise des risques.
- **Ne pas industrialiser un agent sans dispositif de pilotage opérationnel.** Le suivi des performances, la détection des dérives, les tests réguliers, les plans de continuité et l'attribution explicite des responsabilités sont des conditions essentielles de confiance.
- **Ne pas considérer les recommandations d'un agent comme des décisions humaines.** Toute recommandation doit pouvoir être vérifiée, justifiée, tracée et auditée avant d'être utilisée dans un processus décisionnel.

Acte 3

Comment industrialiser l'IA agentique dans un cadre maîtrisé ?

3.1 Pourquoi les projets ne passent pas à l'échelle

Les échanges soulignent l'écart entre un prototype performant et un agent industrialisable. Un POC valide un cas d'usage guidé, mais peine à passer à l'échelle face aux contraintes du run : **boucle agentique instable, absence de télémétrie, risques IT/sécurité** sur des accès sur-permissifs et **dérive des coûts de tokens** liés à la surcharge du contexte (context inflation).

« Il faut d'abord maîtriser l'espace dans lequel l'IA va pouvoir travailler. À l'intérieur de cet univers, chaque usage autonome doit avoir son propre dispositif de maîtrise du risque. »

Florence Picard
Membre agrégé de l'Institut des Actuaires

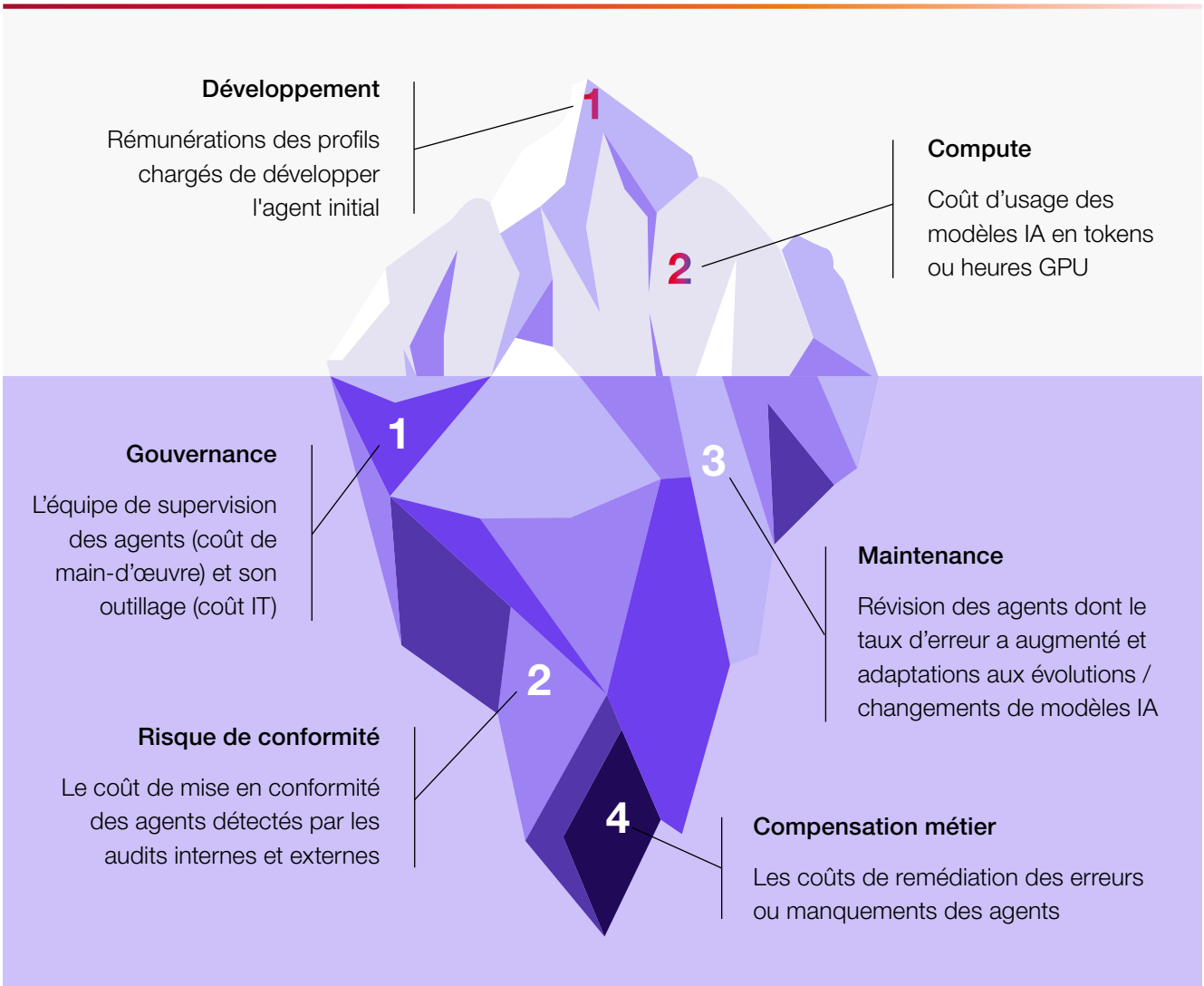
APPORT

Passer à la production exige un standard supérieur structuré autour de quatre exigences :

- **Fiabilité architecturale** : garantir une exécution durable, gérer les conditions d'arrêt et valider chaque tour d'interaction.
- **Rigueur opérationnelle & IT :** imposer un cadre standardisé, assurer une observabilité fine et fournir un environnement d'exécution isolé (sandboxed).
- **Sobriété contextuelle :** privilégier la composition de micro-agents spécialisés (Domain-Specific) plutôt que de gros modèles avec trop d'outils (MCP) ou d'instructions.
- **Viabilité économique :** maîtriser la consommation de tokens en déléguant les sous-tâches à des modèles ciblés et adaptés.

Iceberg du TCO

Total Cost of Ownership (TCO) : le coût réel de l'exploitation d'un agent IA, et pas seulement de sa création



« Lorsqu'un métier voit qu'un autre métier très proche a réussi à adopter l'IA sur un cas d'usage comparable, cela crée naturellement un effet d'entraînement pour passer à l'échelle. »

Ossama Benbouidda
Responsable processus et organisation, Groupe Caisse des Dépôts

Les standards internationaux confirment la nécessité de cette rigueur :

NIST AI RMF (GenAI Profile) : encadre les risques d'alignement et de dérive cognitive tout au long du cycle de vie de l'agent.

ISO/IEC 42001 : apporte le cadre d'un système de management de l'IA (SMIA) axé sur l'observabilité et l'amélioration continue.

DORA : impose la maîtrise des risques informatiques, la résilience opérationnelle et le contrôle des intégrations tierces (outils, API, MCP).

L'industrialisation d'un système agentique se situe précisément à la jonction de ces trois exigences.



3.2 Les familles de freins

Les retours d'expérience montrent que le passage à l'échelle des projets d'IA agentique se heurte généralement à quatre grandes familles d'obstacles : **les limites d'architecture technique** (boucle agentique, exécution durable, isolation), **les enjeux organisationnels**, **les contraintes économiques** (explosion des coûts de tokens par context inflation) et **les exigences de gouvernance**.

Ces dimensions sont indissociables. Une instabilité technique ou une dérive du modèle découle souvent d'une sur-permissivité des accès ou d'une mauvaise isolation ; un rejet par les équipes IT résulte d'une absence de télémétrie ; tandis qu'un modèle économique fragile est la conséquence directe d'un agent monolithique surchargé au lieu d'une architecture composée.

Autrement dit, l'échec ne provient pas de la technologie en soi, mais de la tentative d'industrialiser des démos sans cadre de transformation adapté. Traiter ces freins de manière isolée empêche de bâtir un système viable et sécurisé.

« Le risque d'échec existe à l'échelle de chaque projet, mais le potentiel de gains est trop important pour que les entreprises puissent choisir de ne pas relever ce défi. »

Tang Loaec
Cofondateur, Deepika

APPORT

Pour rendre un écosystème agentique réellement industrialisable, quatre conditions doivent être réunies :

- **Sélectionner les bons cas d'usage :** cibler des processus bien délimités, créateurs de valeur et adaptés à des agents, plutôt que de chercher à créer des agents omnibus voués à l'échec.
- **Installer une gouvernance et une sécurité adaptées :** définir clairement les responsabilités, restreindre le périmètre d'action au strict nécessaire, encadrer les habilitations aux données et maintenir une supervision continue.
- **Structurer l'industrialisation sur une plateforme robuste :** passer du POC à une exploitation robuste reposant sur une orchestration fiable, une télémétrie fine de chaque étape et une gestion sobre de la fenêtre de contexte pour garantir la maîtrise des coûts.
- **Concevoir des agents spécialisés et composables :** renoncer aux agents monolithiques surchargés d'outils et de documentation. L'industrialisation exige de privilégier des agents, orchestrés entre eux avec un contexte minimal, des environnements d'exécution isolés pour garantir la fiabilité et la sobriété budgétaire.

3.3 Les critères d'éligibilité d'un cas d'usage agentique

Les retours d'expérience convergent : l'échec récurrent des projets d'IA agentique découle d'un mauvais ciblage initial. La tentation de créer un système agentique « couteau suisse » capable de gérer un processus de bout en bout conduit systématiquement à l'instabilité et à la surcharge contextuelle. Le cas d'usage idéal ne cherche pas à automatiser un métier dans sa globalité, mais cible des **activités granulaires, fréquentes, semi-structurées et mesurables**. L'enjeu est d'isoler des sous-tâches bien délimitées pouvant être déléguées à des modules spécialisés au sein d'un **système multi-agent**.

« Les collaborateurs ont commencé à automatiser leurs tâches avant même que l'organisation ait eu le temps de mettre en place tout le cadre permettant de piloter la valeur créée. »

Patrick Pansier
Responsable Data, Digital & Innovation, LBP AM

APPORT

Pour garantir le passage du prototype à une exploitation industrielle pérenne, la qualification d'un cas d'usage doit s'appuyer sur une évaluation croisée selon trois familles de critères :

1

Critères métier & économiques

- **Valeur ajoutée mesurable** : le cas d'usage doit apporter un gain clair et évaluable (gain de temps, amélioration de l'expérience client/collaborateur, réduction des erreurs).
- **Fréquence et volumétrie :** cibler des tâches récurrentes dont les coûts de traitement actuels sont identifiés.
- **Justification de l'équation économique :** l'apport métier doit être mis en regard du coût de calcul de la boucle agentique. Le recours à l'IA doit être financièrement viable face à la consommation de tokens, en évitant de mobiliser des modèles généralistes surdimensionnés pour des tâches simples.

2

Critères agentiques (valeur ajoutée de la boucle)

- **Dépassement des approches déterministes :** le besoin ne doit pas pouvoir être résolu par un moteur de règles, un script RPA ou un workflow rigide.
- **Complexité décisionnelle ciblée :** le cas exige un raisonnement multi-étape, la gestion d'exceptions imprévues, ou l'orchestration d'outils distincts (API, bases de données, etc.).
- **Périmètre d'information maîtrisé :** la tâche doit pouvoir s'exécuter dans une fenêtre de contexte restreinte, sans nécessiter la transmission de l'ensemble de la mémoire d'entreprise.



3

Critères d'exploitation & d'architecture

- **Intégration et isolation :** les données source doivent être fiables et accessibles via des API sécurisées. L'exécution de code ou de requêtes doit pouvoir s'effectuer dans un environnement étanche pour protéger le système d'information.
- **Observabilité et télémétrie :** le flux d'exécution doit permettre une traçabilité intégrale (journalisation de chaque étape et appel d'outil) afin de diagnostiquer rapidement les dérives.
- **Gouvernance et réversibilité :** le cas doit intégrer une supervision humaine (Human-in-the-loop), définir un propriétaire métier clair et garantir des conditions d'arrêt sécurisées (stop conditions).
- **Compatibilité multi-agent :** la tâche doit pouvoir s'insérer comme un module indépendant au sein d'une architecture composée, évitant ainsi l'effet de surcharge (context inflation).

Ajustement sectoriel : la pondération de ces critères varie selon la typologie de l'établissement (banque de détail, banque privée, assurance IARD, gestion d'actifs). Les exigences en matière de contrôle des accès aux données, de risques réglementaires et d'impact client orienteront directement le niveau d'autonomie accordé au système multi-agent.

3.4 Transformer en cinq étapes

« Pour industrialiser, il faut penser production dès la conception : résilience, automatisation, mécanismes de secours et fonctionnement sans intervention manuelle quotidienne. »

Patrick Pansier
Responsable Data, Digital & Innovation, LBP AM

« C'est le Far West » (It's a mess out there) : aujourd'hui, fabriquer des agents robustes reste extrêmement complexe. Il n'existe encore **aucun standard universel** de conception, la télémétrie et l'observabilité s'avèrent très difficiles à l'échelle, et les agents actuels ne sont **ni portables ni composables.**

Face à ce manque de maturité de l'écosystème, réussir l'industrialisation exige de sortir du bricolage pour adopter une démarche structurée. Bien que les méthodes de transformation s'adaptent au cas par cas selon la nature de chaque projet, on distingue néanmoins 5 étapes indispensables :

1

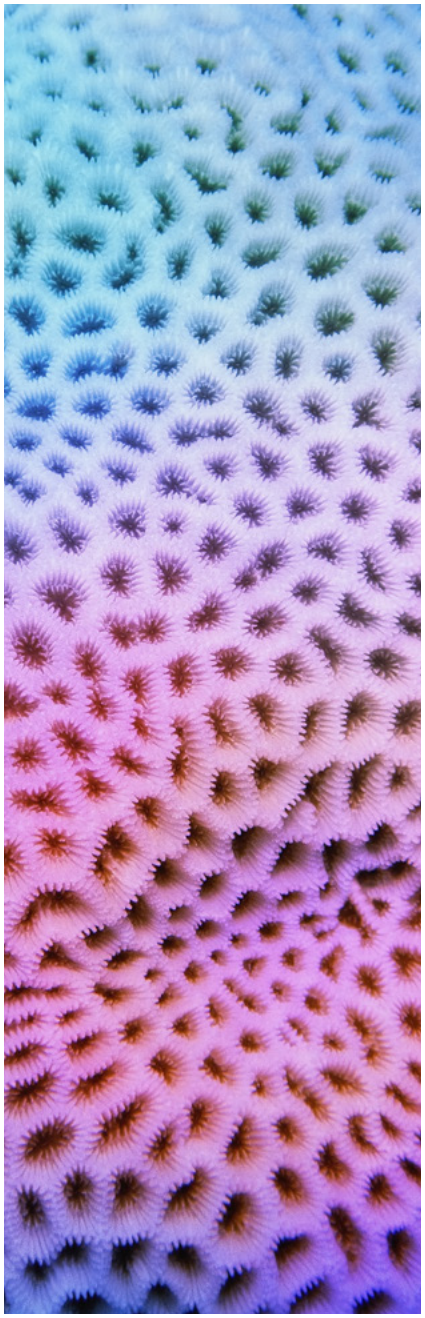
Cadrer et qualifier

Objectif : clarifier le problème métier, le périmètre, les utilisateurs, le niveau de risque, la valeur attendue et le niveau d'autonomie envisageable. La qualification doit **dépasser l'approche monolithique :** quelle tâche ou sous-processus précis voulons-nous transformer ? Quel est le coût de traitement actuel face au coût attendu en tokens ? Quelles données sont nécessaires ? Quelles décisions restent strictement humaines ?

2

Modéliser le parcours et décomposer le processus

Objectif : comprendre le travail réel avant d'automatiser le travail prescrit. L'agentique doit s'insérer dans un processus repensé et **découpé de manière granulaire :** plutôt que de créer un agent « couteau suisse », il s'agit d'isoler les sous-tâches, les exceptions, les points de contrôle, les décisions intermédiaires, les documents et les systèmes sollicités. C'est l'étape clé pour déterminer les périmètres d'action des futurs agents.



3

Concevoir l'architecture du système multi-agent

Objectif : définir la structure du **système multi-agent composé** en évitant le piège de la surcharge contextuelle. Déterminer précisément ce que l'on demande à chaque agent (chercher une information, résumer, orienter une demande, vérifier une règle, générer un document, alerter en cas de problème). Pour chaque agent, la conception fixe ses règles du jeu : les outils qu'il a le droit d'utiliser, les données auxquelles il a accès, ce qu'il doit produire, ainsi que ses limites de sécurité et ses conditions d'arrêt.

4

Évaluer, tester et optimiser

Objectif : mesurer la performance métier, l'efficience économique et la robustesse technique avant déploiement. Les tests doivent évaluer les cas nominaux, les exceptions, les injections adverses, les pannes d'API, les dérives cognitives et les scénarios de débrayage. L'optimisation vise à valider que le système multi-agent maintient un taux d'erreur bas et une consommation de tokens maîtrisée par rapport à un modèle monolithique.

5

Industrialiser, gouverner et piloter

Objectif : exploiter et maintenir le système multi-agent dans la durée. L'industrialisation repose sur **l'exécution durable** (capacité à reprendre après une panne), la télémétrie fine de chaque tour d'interaction, le suivi des coûts en temps réel, les journaux d'audit, le contrôle continu des droits d'accès et l'amélioration continue. Un système multi-agent est un composant vivant du SI qui s'administre via une démarche AgentOps structurée.

3.5 Gouverner un agent comme un collaborateur

Les ateliers posent une question simple : qui est responsable ? Cette question n'a pas une seule réponse. Le développeur, l'intégrateur, le fournisseur, le métier utilisateur, le responsable conformité, le data owner et l'owner de l'agent interviennent à des moments différents. La responsabilité doit donc être distribuée, mais non diluée.

Il n'existe pas de règle universelle : le modèle de gouvernance s'adapte au cas par cas selon l'organisation. Néanmoins, pour éliminer les zones d'ombre, **deux points d'ancrage essentiels** doivent être fixés :

- **Comment superviser les décisions et les risques ?** Fixer le cadre opérationnel de contrôle des actions, le suivi des dérives et le rôle du validateur humain (Human-in-the-loop).
- **Comment valider les évolutions ?** Définir clairement qui autorise les mises à jour de modèles, la modification des règles agentiques ou l'ajout de nouvelles fonctionnalités.

APPORT

Le modèle recommandé est celui d'un agent comme acteur opérationnel. Comme un collaborateur, il a une fiche de poste, un manager, un périmètre, des habilitations, des objectifs, des limites, une revue de performance, une procédure d'escalade et une possibilité de retrait. La différence est qu'il nécessite en plus une surveillance technique continue et une traçabilité exhaustive.

« Un agent IA doit avoir un périmètre aussi clair qu'une fiche de poste : ce qu'il peut faire, les applications auxquelles il peut accéder et les responsabilités qu'il ne doit pas exercer. »

Ossama Benbouidda

Responsable processus et organisation, Groupe Caisse des Dépôts

Contrairement à un collaborateur humain, l'agent exige en complément des garde-fous d'ingénierie stricts :

1. **Une surveillance technique et une télémétrie continue :**
   Traçabilité intégrale (logs) de chaque décision, appel d'API et échange entre micro-agents pour détecter immédiatement toute dérive.

2. **Un environnement d'exécution étanche (Sandboxing) :**
   Isolation des accès aux systèmes d'information pour prévenir les actions involontaires.

3. **Une procédure d'arrêt d'urgence (Stop conditions) :**
   Capacité à couper l'exécution de manière déterministe en cas de comportement anormal.



Qui est responsable d'un agent IA autonome ?

Une responsabilité distribuée, mais jamais diluée

L'AGENT EST TRAITÉ COMME UN COLLABORATEUR NUMÉRIQUE

Owner de l'agent

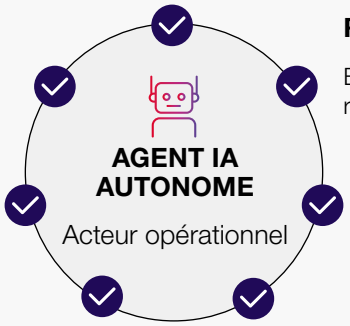
Responsable du cycle de vie de l'agent et de sa performance. Décide, arbitre, rend compte.

Sponsor métier

Définit la valeur métier, priorise et alloue les moyens.

Risques & Conformité

Évalue les risques, définit le cadre réglementaire et contrôle la conformité.



Data Owner

Garantit la qualité, la disponibilité et l'usage éthique des données.

Utilisateurs métier

Utilisent l'agent dans leur activité et remontent les anomalies et améliorations.

Fournisseur / Développeur / Intégrateur

Conçoit, développe et intègre l'agent. Garantit la conformité technique.

IT/AgentOps

Exploite, supervise techniquement et garantit la disponibilité, la sécurité et la traçabilité.

RESPONSABILITÉS DE L'AGENT

Fiche de poste	Périmètre d'action	Habilitations	Objectifs	Limites	Escalade	Revue de performance	Possibilité de retrait

EXIGENCES SPÉCIFIQUES IA

Monitoring continu

Surveillance en temps réel du comportement et des performances.

Traçabilité exhaustive

Journalisation complète des décisions, actions et données utilisées.

Audit

Vérifications régulières et preuve de conformité sur l'ensemble du cycle de vie.

Supervision technique

Contrôle de la résilience, de la sécurité et de la qualité opérationnelle.

Aucun acteur n'est seul responsable	Chacun est responsable de son domaine de décision	La gouvernance consiste à organiser cette responsabilité de bout en bout.

3.6 Mesurer la performance et maintenir la confiance

APPORT

La mise en production d'un agent ne constitue pas l'aboutissement du projet, mais le début de son exploitation. Contrairement à une application traditionnelle, un agent évolue dans un environnement dynamique : les modèles changent, les données se transforment, les outils auxquels il accède évoluent et les usages se diversifient. Sa performance ne peut donc être considérée comme acquise.

Le pilotage ne consiste plus seulement à mesurer des indicateurs de performance, mais à vérifier en permanence que l'agent reste digne de confiance. **Cette confiance repose sur un équilibre entre cinq dimensions complémentaires : la valeur créée pour le métier, la qualité des décisions produites, la maîtrise des risques, la soutenabilité économique et l'appropriation par les utilisateurs.** La dégradation d'une seule de ces dimensions suffit souvent à remettre en cause l'ensemble du dispositif.

Les organisations les plus matures ne suivent donc pas uniquement des KPI techniques. Elles mettent en place un véritable tableau de bord de confiance permettant d'identifier les dérives, d'ajuster le niveau d'autonomie des agents et de décider, lorsque cela est nécessaire, d'un retour à une supervision humaine.



« La confiance ne se décrète pas : elle se construit progressivement, à mesure que l'on observe ce que l'agent sait réellement faire et que l'on sécurise ses comportements. »

Guy-Matthieu Verwaerde
CEO et Cofondateur, StudyAssur

Dimension	Question à se poser	Exemples d'indicateurs
Valeur métier	L'agent crée-t-il réellement de la valeur ?	Temps gagné, taux de traitement, satisfaction, qualité
Fiabilité	Peut-on continuer à lui faire confiance ?	Exactitude, hallucinations, escalades, stabilité
Risque	Respecte-t-il les règles fixées ?	Violations, incidents, blocages, interventions humaines
Économie	Le modèle reste-t-il rentable ?	Coût par dossier, coût de supervision, TCO
Adoption	Les utilisateurs l'utilisent-ils et lui font-ils confiance ?	Usage réel, contestations, feedback, satisfaction



« Une démonstration peut être techniquement convaincante sans avoir réellement de sens pour le métier auquel elle est censée s'appliquer. »

Tang Loaec
Cofondateur, Deepika

Pour garantir cet équilibre, les organisations qui industrialisent l'IA agentique doivent déployer un tableau de bord de confiance articulé autour d'un pilotage à deux niveaux :

1

Pilotage métier & économique (valeur, qualité et usages)

- **Qualité des décisions et valeur créée :** évaluation du taux de succès des tâches, de la pertinence des résultats et des gains de productivité réellement perçus par le métier.
- **Supervision et niveau d'autonomie :** suivi du taux de recours au validateur humain (Human-in-the-loop), taux d'acceptation des recommandations de l'agent et fréquence des escalades vers les experts.
- **Soutenabilité financière :** contrôle en temps réel de la consommation de tokens et du coût de calcul par transaction, pour s'assurer que la valeur générée dépasse l'investissement d'infrastructure.

2

Pilotage technique & opérationnel (sécurité, risques et observabilité)

- **Télémétrie fine et traçabilité :** capture exhaustive des logs à chaque étape du raisonnement, des requêtes exécutées et des échanges entre micro-agents pour garantir une **auditabilité totale**.
- **Détection des dérives (Going off the rails) :** identification rapide des hallucinations, des pertes de contexte ou des comportements anormaux avant qu'ils ne touchent les systèmes clients.
- **Garde-fous déterministes :** application stricte des conditions d'arrêt (stop conditions) et des limites de requêtes pour bloquer immédiatement un agent en cas de comportement à risque.

Les organisations les plus matures dépassent ainsi le simple tableau de bord de production. Grâce à ce tableau de bord de confiance à deux niveaux, elles disposent des leviers nécessaires pour identifier les dérives, ajuster le périmètre d'action des agents et déterminer à tout moment si leur niveau d'autonomie peut être maintenu, renforcé ou, au contraire, réduit vers une supervision humaine.

« Délimiter précisément le périmètre d'un agent permet aussi de rassurer : même s'il paraît omniscient, il reste un acteur avec un rôle et un champ d'action clairement définis. »

Ossama Benbouidda
Responsable processus et organisation, Groupe Caisse des Dépôts

3.7 Sécurité et résilience : le changement de surface d'attaque

APPORT

Dès qu'un agent peut agir, la sécurité ne porte plus seulement sur la confidentialité d'une donnée ou la robustesse d'un modèle. Elle porte sur les outils que l'agent peut appeler, les actions qu'il peut déclencher, la mémoire qu'il conserve, les agents avec lesquels il coopère, les instructions qu'il peut recevoir et les chemins de contournement possibles. Les cadres OWASP dédiés aux applications LLM et agentiques rappellent que l'agent transforme la nature du risque : la sortie du modèle n'est plus seulement un texte, elle peut devenir une action.

Les exigences DORA sur la résilience opérationnelle numérique renforcent l'attention portée au risque ICT, aux tiers, aux tests de résilience, à la gestion des incidents et à la continuité. Une application agentique connectée à des processus financiers doit donc être traitée comme un composant critique dès lors qu'elle influe sur un service, un flux, un contrôle ou une décision.



Plus un agent gagne en autonomie et en impact sur le métier, plus son pilotage devient critique. L'industrialisation ne consiste donc pas à libérer l'agent du contrôle, mais à rendre le contrôle compatible avec la vitesse et le volume.

« La confiance repose moins sur une validation humaine permanente que sur la capacité à détecter les écarts, à auditer les décisions et à faire évoluer les règles de l'agent. »

Tang Loaec
Cofondateur, Deepika

Acte 4

Quelle conduite du changement et quelle feuille de route de transformation ?

Comment faire adopter durablement des agents dans des organisations où la responsabilité reste humaine ?

4.1 Pourquoi la conduite du changement devient critique

L'IA agentique affecte à la fois les pratiques opérationnelles, les responsabilités, les statuts et les représentations du travail. Si elle permet de faire gagner du temps, elle peut aussi déplacer la charge cognitive vers la supervision. Elle peut améliorer la qualité, mais elle peut aussi produire une confiance excessive dans les recommandations. Elle peut augmenter les métiers, mais elle peut aussi nourrir une crainte de remplacement. La conduite du changement doit donc traiter à la fois la compétence, la confiance, l'acceptabilité sociale et la responsabilité.

APPORT

Une erreur fréquente consiste à former les utilisateurs à l'usage de l'outil sans adapter les processus de travail. La maîtrise des techniques de formulation des requêtes ne constitue qu'une première étape. Les collaborateurs doivent également comprendre les capacités et les limites de l'agent, connaître les situations dans lesquelles ses recommandations doivent être remises en question, savoir documenter les corrections apportées, déclencher une procédure d'escalade lorsque cela est nécessaire et signaler tout incident conformément aux dispositifs de gouvernance en place.

« L'industrialisation de l'IA agentique suppose de faire émerger une fonction qui n'existe pas encore pleinement : celle qui assure l'interface entre les technologies IA et les métiers. »

Jean-Michel Ghidaglia
Cofondateur, Deepika

La conduite du changement doit accompagner l'évolution de la gouvernance au fur et à mesure de la progression de la maturité de l'IA agentique. Dans ce cadre, un IA Office peut constituer la structure de pilotage clé pour assurer une gouvernance cohérente des initiatives d'IA. Il définit la stratégie IA, priorise le portefeuille de cas d'usage, établit les standards techniques et méthodologiques et veille au respect des exigences réglementaires, éthiques et de cybersécurité. Il pilote également le cycle de vie des agents IA, les indicateurs de performance, la gestion des risques et les dispositifs de contrôle. Il a également la charge de définir et coordonner les actions de conduite du changement afin de garantir une adoption maîtrisée et une création de valeur durable.

Gouvernance et conduite du changement

Deux trajectoires indissociables pour atteindre la maturité

	 **GOUVERNANCE** Ce que l'organisation doit être capable de gouverner	 **CONDUITE DU CHANGEMENT** Ce que l'organisation doit faire évoluer
NIVEAU 1	**Gouverner les modèles IA** IA assistante	**Acculturer et rassurer**
NIVEAU 2	**Gouverner les agents IA** IA agentique	**Transformer les pratiques de travail**
NIVEAU 3	**Gouverner un écosystème d'agents** Organisation augmentée	**Transformer durablement l'organisation**

Expertise



Florence Picard
Membre agrégé de l'Institut des Actuaires, docteure en mathématiques, experte des risques, en assurance et en finance

« Le véritable danger serait de perdre confiance dans l'être humain. »

L'IA agentique marque un changement de nature : d'un simple assistant, elle devient progressivement capable de prendre en charge des tâches auparavant confiées à des collaborateurs expérimentés.

Cette évolution ne doit pourtant pas conduire à surestimer la machine. L'autonomie d'un agent doit rester encadrée, comme l'est celle d'un collaborateur humain : règles de fonctionnement, contrôle et supervision doivent être adaptés à chaque usage et au niveau de risque associé, et garantir la piste d'audit.

L'un des enjeux les plus sensibles concerne la transmission des compétences. Les tâches aujourd'hui automatisables étaient aussi celles par lesquelles les juniors apprenaient leur métier, confrontaient la théorie au réel et développaient progressivement leur jugement et leur intuition. Gagner en productivité à court terme ne doit donc pas conduire à fragiliser le patrimoine de compétences de l'entreprise.

Paradoxalement, cette transformation peut permettre à certains métiers de retrouver leur vocation première. Pour l'actuaire, l'automatisation des travaux calculatoires peut libérer du temps pour revenir au cœur du métier : comprendre, anticiper et maîtriser les risques.

Mais l'IA ne peut pas être pensée isolément. Son développement se combinera avec d'autres mutations : blockchain, évolution des paiements et des infrastructures de marché, changement climatique, tensions géopolitiques, disponibilité des semi-conducteurs, consommation d'énergie et de ressources.

Le véritable enjeu est de profiter de la puissance de l'IA sans perdre ni notre capacité de jugement et esprit critique, ni notre capacité à transmettre, sans oublier les limites du monde dans lequel elle s'inscrit.

La transformation agentique est donc autant un sujet de technologie que de gouvernance, de compétences et de responsabilité. Le risque principal ne serait pas de faire trop confiance à l'IA, mais de finir par ne plus faire suffisamment confiance à l'être humain.

4.2 Les publics à accompagner

Le développement de l'IA agentique requiert un accompagnement spécifique pour chaque population de l'organisation. Les enjeux, les compétences à acquérir et les modalités d'accompagnement diffèrent selon les responsabilités de chacun.

Pour la Direction générale, la priorité consiste à identifier les domaines où l'IA crée de la valeur tout en maîtrisant les risques associés. Les dirigeants doivent développer des compétences d'arbitrage entre création de valeur et exposition aux risques, comprendre les enjeux de souveraineté, piloter un portefeuille de cas d'usage et définir les lignes rouges encadrant les usages de l'IA. Cet accompagnement peut prendre la forme de séminaires exécutifs et de comités IA permettant d'éclairer les décisions stratégiques.

Pour les métiers, l'enjeu est d'intégrer les agents IA dans les activités quotidiennes sans perdre la maîtrise des processus. Les collaborateurs doivent apprendre à qualifier les activités pouvant être confiées à un agent, organiser la supervision humaine, contester les résultats lorsque cela est nécessaire et produire un retour d'expérience afin d'améliorer les solutions. Des ateliers centrés sur les processus métiers et des formations construites autour de cas d'usage concrets peuvent permettre de développer ces compétences.



Pour les managers, l'arrivée de collaborateurs assistés par l'IA modifie les pratiques de pilotage. Ils doivent être en mesure de gérer la capacité de leurs équipes, d'évaluer la qualité des productions, de mettre en place des mécanismes de contrôle et de favoriser l'adoption des nouveaux outils. Des rituels de pilotage adaptés et des tableaux de bord intégrant les indicateurs liés à l'IA constituent les principaux leviers d'accompagnement.

Pour les fonctions Risques et Conformité, l'objectif est de disposer des moyens nécessaires pour auditer les agents IA et démontrer leur conformité. Les compétences attendues portent sur la définition des exigences, la collecte des preuves, l'exploitation des journaux d'exécution, l'analyse des explications produites par les systèmes et la réalisation de tests. Des revues de conception, des contrôles réguliers et des audits permettent de structurer cette démarche.



Pour les équipes IT, Data et Sécurité, l'enjeu est d'exploiter les agents IA dans un cadre robuste, sécurisé et gouverné. Cela suppose de développer des compétences en AgentOps, en observabilité des agents, en cybersécurité et en gouvernance des données. La mise en œuvre repose sur des runbooks opérationnels, des campagnes de tests, des exercices de red teaming et des dispositifs de supervision continue afin de garantir la fiabilité et la résilience des solutions déployées.

Enfin, **pour les Ressources humaines,** l'IA soulève des questions d'évolution des métiers et des compétences. Il est nécessaire de cartographier les compétences actuelles, d'identifier les besoins de montée en compétences ou de mobilité et de mesurer l'acceptabilité des transformations. Une communication transparente, des parcours de développement ou de reconversion ainsi qu'un dialogue social régulier doivent permettre d'accompagner ces évolutions et de favoriser leur appropriation par les collaborateurs.

Au-delà des actions propres à chaque population, la démarche de conduite du changement vise à construire une culture commune de l'IA, fondée sur la maîtrise des risques, la création de valeur et la responsabilisation de l'ensemble des acteurs.

« Si l'IA remplace les tâches par lesquelles les juniors apprenaient leur métier, il faut repenser la manière dont nous formerons les experts de demain. »

Florence Picard
Membre agrégé de l'Institut des Actuaires

4.3 Le modèle d'adoption : une confiance graduée

APPORT

L'adoption de l'IA agentique doit suivre une logique de confiance graduée. L'agent commence comme stagiaire numérique sur un périmètre étroit, sans action irréversible. L'agent gagne ensuite des droits lorsqu'il démontre sa fiabilité, sa stabilité, sa valeur, sa capacité à expliquer et sa capacité à déclencher une escalade. Cette démarche progressive présente l'avantage d'être à la fois plus acceptable pour les utilisateurs et plus robuste pour les fonctions de contrôle.



« Je ne suis pas pessimiste sur la place de l'humain, à condition de ne pas surestimer la valeur de la rationalité de l'IA. Dans notre monde d'incertitude, cela reviendrait à sous-estimer la valeur des humains dans leur aptitude à envisager l'improbable, et à se soumettre aux algorithmes enfermés dans les data. »

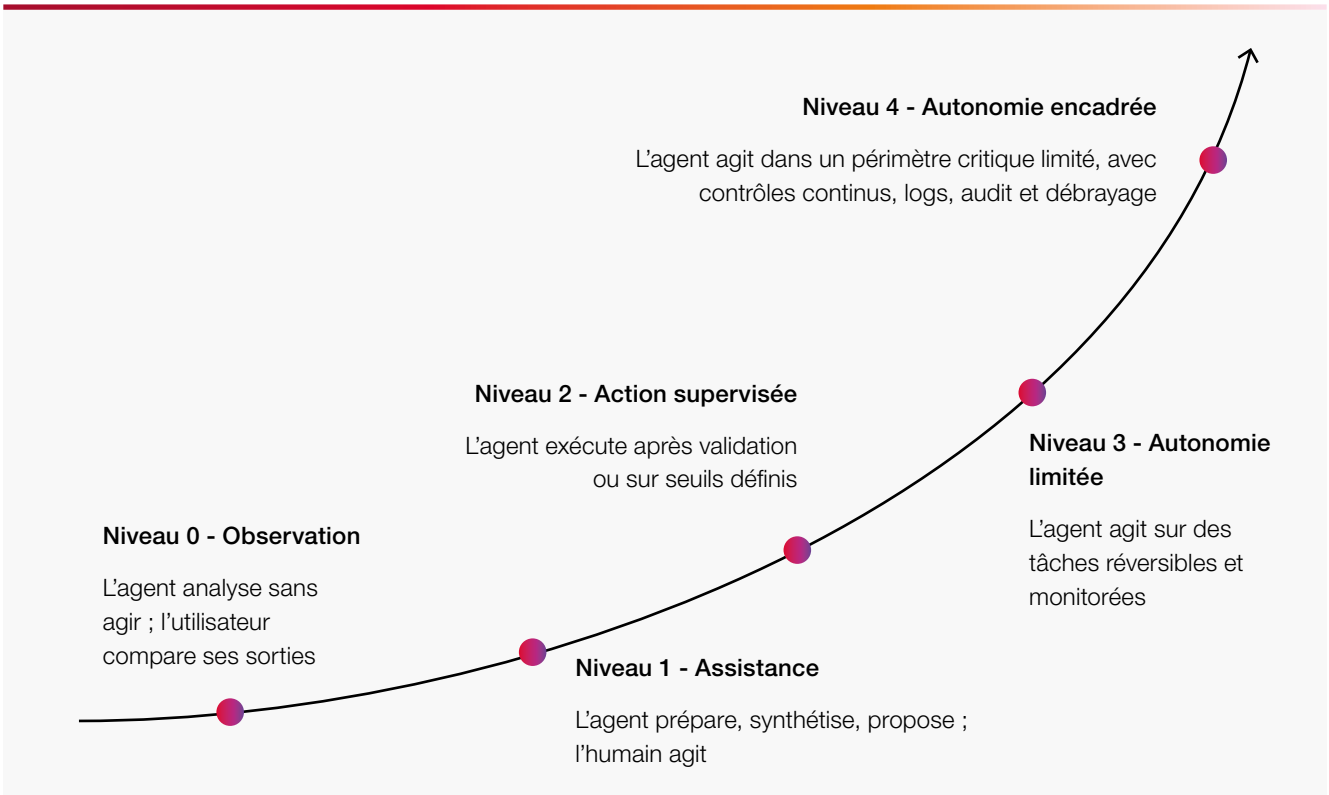
Florence Picard
Membre agrégé de l'Institut des Actuaires



« À terme, on peut imaginer des agents capables de modéliser et de répliquer certains styles de gestion, tout en restant sous la surveillance d'un gérant. »

Patrick Pansier
Responsable Data, Digital & Innovation, LBP AM

Une démarche de confiance graduée



4.4 Le dialogue social et la vérité sur la valeur

APPORT

L'accompagnement du déploiement de l'IA agentique doit reposer sur un principe de transparence. Il convient de donner une vision claire des objectifs poursuivis, des bénéfices attendus et des impacts identifiés sur les activités, les métiers et les compétences. Le discours d'adoption doit éviter deux écueils : présenter l'IA agentique comme une technologie sans effet sur le travail ou, à l'inverse, l'associer exclusivement à une logique de réduction des effectifs. Si les premiers bénéfices perçus concernent le gain de temps, l'amélioration de la qualité et l'augmentation des capacités de traitement, les questions relatives à l'évolution des emplois et des organisations doivent néanmoins être abordées de manière explicite, à partir d'une cartographie des activités, d'une analyse des compétences impactées et d'un plan de montée en valeur sur les rôles humains à développer.

Cette démarche s'appuie sur une communication régulière et pédagogique afin de rendre accessibles les concepts liés à l'IA agentique, d'expliquer les choix de gouvernance et de partager l'avancement des travaux. La vulgarisation des enjeux techniques, organisationnels et réglementaires favorise une compréhension commune et contribue à instaurer un climat de confiance.



L'association des représentants du personnel à la démarche et l'intervention dans les instances doivent permettre d'éclairer les impacts de la transformation. Le dialogue social doit porter notamment sur l'identification des tâches automatisées, des activités augmentées par l'IA et des activités qui demeurent sous responsabilité humaine. Il doit également aborder les nouvelles responsabilités liées à l'utilisation des agents IA, les modalités de supervision et de contrôle, les garanties apportées aux collaborateurs, les critères d'évaluation de la performance ainsi que les dispositifs de développement des compétences, de mobilité et de reconversion. L'objectif est de construire un cadre partagé pour l'intégration des agents IA, fondé sur la visibilité des décisions, la transparence des impacts et l'accompagnement des transformations des métiers.

« L'adoption de l'IA ne se décrète pas : elle s'anime. Formation, webinaires, communication et retours du terrain permettent d'accompagner ceux qui démarrent et d'identifier ceux qui sont déjà en avance. »

Patrick Pansier
Responsable Data, Digital & Innovation, LBP AM

4.5 Feuille de route de transformation

Le déploiement de l'IA agentique s'inscrit dans une trajectoire de transformation progressive.

Une première phase de cadrage permet de définir l'ambition, les principes de gouvernance, les cas d'usage prioritaires et la grille de sélection valeur/risque/production. Lors de cette phase initiale sont également posés les rôles et responsabilités (sponsors, owners), les comités de gouvernance et les règles d'utilisation (lignes rouges : décisions sensibles, données interdites, actions irréversibles).

Dans un second temps, **les premières expérimentations** portent sur un nombre limité de cas d'usage, ciblés sur des tâches fréquentes, semi-structurées et mesurables, afin de mesurer la valeur créée, d'évaluer les risques, de valider les modalités de supervision humaine, d'évaluer la qualité des données, de former les premiers utilisateurs et de construire les premiers retours d'expérience.

La phase d'industrialisation vise ensuite à mettre en place les capacités opérationnelles nécessaires à un passage à l'échelle : fondations AgentOps (monitoring, logs, runbooks, gestion des versions), modèle RACI, contrôles conformité, sécurité et protection des données, suivi des coûts complets (tokens, supervision, run, maintenance), organisation de la montée en compétences de différents acteurs et création d'un protocole de débrayage et de décommissionnement.

Enfin, la généralisation s'appuie sur une gouvernance pérenne, l'intégration des agents dans les processus métiers, le pilotage de la valeur, l'amélioration continue et l'accompagnement des transformations des métiers et des compétences, en associant les parties prenantes et les représentants du personnel.

« L'enjeu n'est pas de mettre de l'IA partout, mais de modéliser, cartographier et optimiser les processus avant de décider où la technologie apporte réellement de la valeur. »

Ossama Benbouidda
Responsable processus et organisation,
Groupe Caisse des Dépôts

« L'IA agentique ne doit pas être traitée comme un projet exclusivement technologique : son industrialisation commence par la compréhension du besoin métier. »

Jean-Michel Ghidaglia
Cofondateur, Deepika



« Dans dix ans,
la question ne sera
peut-être plus seulement
de savoir comment l'IA
transforme nos métiers,
mais comment elle
transforme la manière
même de consommer
les produits financiers. »

Patrick Pansier
Responsable Data, Digital & Innovation, LBP AM

Conclusion générale

De la puissance à la confiance

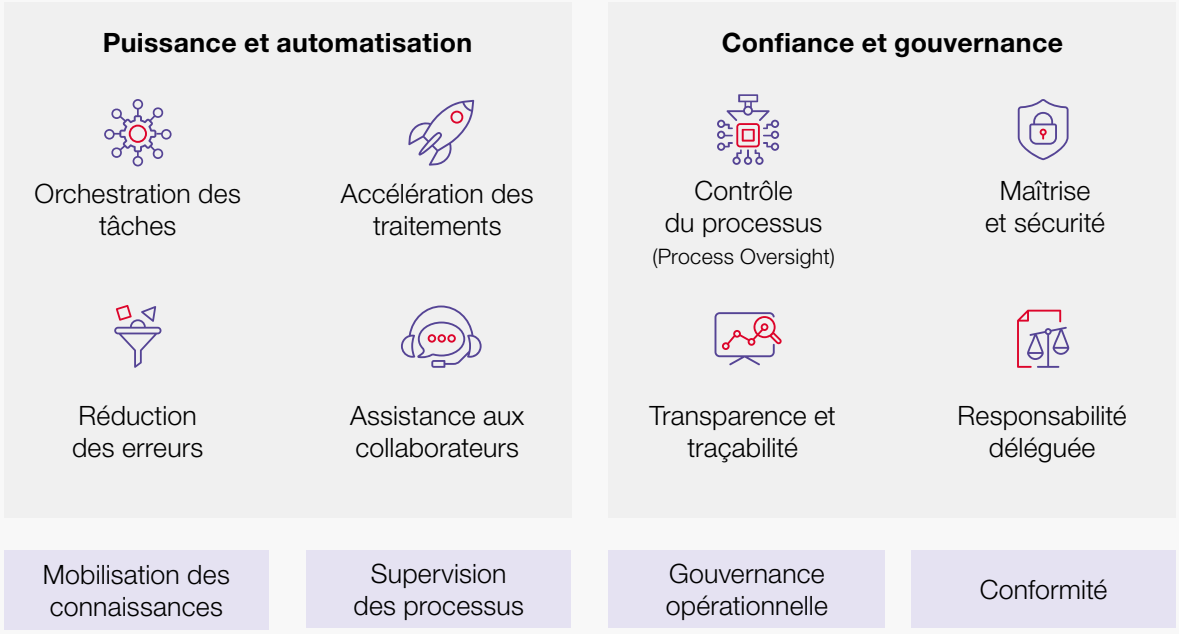
L'IA agentique marque une nouvelle étape dans la transformation des secteurs bancaire et assurantiel. Elle offre des perspectives inédites en permettant d'orchestrer des tâches, de mobiliser des connaissances, d'accélérer les traitements, de superviser des processus, de réduire les erreurs ou les oublis et d'assister les collaborateurs dans leurs activités. Toutefois, elle redéfinit également la nature des risques. Tant qu'un système d'IA se limite à produire un contenu, le contrôle porte principalement sur la qualité et la pertinence de la réponse. En revanche, dès lors qu'un agent prépare une décision, mobilise des outils ou déclenche une action, le contrôle ne concerne plus seulement le résultat produit, mais l'ensemble du processus qui y conduit.

Les ateliers mettent en évidence un niveau de maturité élevé dans la perception des usages de l'IA agentique. Les participants ne visent pas une automatisation généralisée des activités bancaires ou assurantielles ; ils privilégient des cas d'usage dans lesquels les agents apportent une valeur ajoutée tangible en allégeant la charge de travail, en accélérant l'accès à l'information, en renforçant les dispositifs de contrôle et en facilitant le partage des connaissances. Ils reconnaissent l'intérêt d'agents capables d'assister, d'anticiper, de collaborer et d'agir par délégation dans un cadre défini. En revanche, ils rejettent les usages susceptibles de conduire à une manipulation des utilisateurs, à des décisions sensibles dépourvues de supervision humaine, à l'effacement du rôle du collaborateur, ainsi qu'à toute forme d'opacité ou de défaut de traçabilité.

La thèse défendue dans ce livre blanc est la suivante : les secteurs bancaire et assurantiel n'ont pas besoin d'une IA agentique spectaculaire, mais d'une IA agentique gouvernable. La valeur ne résidera pas dans un degré d'autonomie toujours plus élevé, mais dans la capacité à déployer des agents dont l'autonomie est utile, maîtrisée, mesurable, explicable, réversible et acceptée. Dès lors, la véritable question n'est plus : jusqu'où pouvons-nous automatiser ? Elle devient : *quelles responsabilités sommes-nous en mesure de déléguer tout en conservant un niveau de maîtrise compatible avec nos exigences de gouvernance, de conformité et de confiance ?*

Le succès de l'IA agentique reposera sur la capacité des organisations à articuler quatre leviers complémentaires : une sélection rigoureuse des cas d'usage, une industrialisation maîtrisée, une gouvernance opérationnelle robuste et une conduite du changement ambitieuse. À défaut, elles risquent de multiplier des prototypes prometteurs, mais difficiles à pérenniser, coûteux à maintenir et insuffisamment maîtrisés. Dans ces secteurs où la confiance constitue un actif essentiel, la véritable promesse de l'IA agentique n'est pas de se substituer à l'humain, mais de renforcer sa capacité d'analyse, de libérer du temps pour les tâches à forte valeur ajoutée et de lui fournir les éléments nécessaires pour prendre des décisions plus éclairées.

De la puissance à la confiance



La véritable promesse de l'IA agentique : renforcer l'humain pour des décisions éclairées dans un cadre de confiance

Expertise



Stéphane Houin
Vice-Président
Expert en charge des offres digitales & IA pour les Services Financiers, CGI

Saisir la rupture de nature : le grand déplacement

Ces deux dernières années, l'IA générative s'est principalement imposée comme une technologie d'assistance : résumer un document, rechercher une information, produire un contenu ou préparer une réponse. L'IA agentique introduit une rupture d'une autre nature. **Nous passons d'une IA qui répond à une IA qui agit.** Un agent peut planifier une séquence d'actions, mobiliser plusieurs outils, interagir avec le système d'information, contrôler un résultat et adapter son comportement pour atteindre un objectif.

Dans la banque et l'assurance, ce déplacement change profondément la nature du risque. L'enjeu n'est plus seulement de vérifier la pertinence d'une réponse générée, mais de maîtriser **la qualité et les conséquences d'une action préparée ou exécutée**. Dès lors que l'IA entre dans les processus opérationnels, elle doit répondre à un nouveau contrat de confiance : autonomie, certes, mais autonomie observable, explicable, réversible et gouvernable.

Sortir du mirage des prototypes

Le marché connaît aujourd'hui une multiplication des POC agentiques. Leur réussite peut cependant être trompeuse. Un agent performant dans un environnement guidé, sur quelques scénarios maîtrisés, ne préjuge ni de sa robustesse en production ni de son équation économique à grande échelle.

L'industrialisation révèle un **TCO agentique** souvent sous-estimé : multiplication des appels aux modèles, inflation du contexte (context inflation), instabilité des boucles de raisonnement et d'action, maintenance des prompts et des outils, gestion des exceptions, observabilité et télémétrie. À l'échelle de milliers ou de millions d'opérations, quelques secondes de latence, quelques appels supplémentaires ou un faible taux d'échec deviennent des sujets industriels et financiers.

C'est pourquoi le modèle de l'agent monolithique « couteau suisse », capable théoriquement de tout faire, constitue selon nous une impasse. **L'avenir industriel appartient davantage à des architectures composées de micro-agents spécialisés**, aux responsabilités délimitées, orchestrés et supervisés au sein d'un cadre de télémétrie commun. Cette spécialisation facilite les tests, la maîtrise des habilitations, l'explicabilité, le suivi des coûts et le remplacement d'un composant sans remettre en cause l'ensemble de la chaîne.

Construire le cadre de confiance

L'autonomie ne signifie pas l'abandon du contrôle. Dans les services financiers, elle doit s'arrêter là où commencent la responsabilité juridique, la protection du client et la sécurité opérationnelle.

Cela impose des lignes rouges : **aucune décision juridiquement ou réglementairement engageante ne doit être déléguée sans le niveau approprié de validation humaine ; aucune interaction client autonome sensible ne doit échapper à la**



supervision ; aucun agent ne doit accéder à un processus critique sans habilitations strictement délimitées, cloisonnement et mécanismes d'arrêt d'urgence. DORA, l'AI Act et les exigences des autorités comme la CNIL ou l'ACPR renforcent cette nécessité d'une gouvernance intégrée dès la conception.

Une règle simple peut guider cette transformation : **encadrer l'autonomie d'un agent comme on définit le cadre de responsabilité** d'un collaborateur. Chaque agent devrait disposer d'une véritable « fiche de poste » précisant sa mission, ses objectifs, ses données accessibles, ses outils, ses droits d'action, ses interdictions et ses conditions d'escalade. Et surtout, chaque agent doit avoir un responsable humain clairement identifié : un **Agent Owner**, comptable de son usage et de sa performance opérationnelle.

Industrialiser par la méthode et la confiance graduée

Le passage à l'échelle ne peut donc être traité comme un simple projet informatique. Il suppose une démarche industrielle en cinq temps : **qualifier finement le cas d'usage ; définir le niveau d'autonomie acceptable ; concevoir et tester l'architecture agentique ; sécuriser son intégration au SI ; puis l'exploiter dans une démarche AgentOps**, avec supervision continue des performances, coûts, dérives et incidents.

Cette discipline technique doit s'accompagner d'une discipline d'adoption. Nous proposons pour cela le principe de **confiance graduée**. Un agent entre dans l'organisation comme un « stagiaire numérique » : périmètre limité, actions réversibles, supervision forte. À mesure qu'il démontre sa fiabilité, sa stabilité et son explicabilité, son autonomie peut progresser. Les droits ne sont donc pas accordés sur la promesse technologique, mais **gagnés par la preuve opérationnelle**.

Conclusion : l'humain, chef d'orchestre de l'organisation augmentée

La banque et l'assurance n'ont pas besoin d'une IA agentique spectaculaire. Elles ont besoin d'une **IA agentique gouvernable, industrialisable et économiquement soutenable**.

L'objectif n'est pas d'effacer l'humain du processus. En confiant à des collectifs d'agents spécialisés la préparation documentaire, les contrôles de premier niveau, la collecte d'informations ou certaines pré-analyses, nous pouvons au contraire repositionner le collaborateur là où sa valeur est la plus forte : arbitrer, contextualiser, décider et assumer la responsabilité.

Dans l'organisation financière augmentée, l'IA agit davantage ; l'humain ne compte pas moins. Il devient le chef d'orchestre du processus et le garant ultime de la décision.

Expertise



Barbara Rallu
Vice-Présidente Transformation des organisations & Change Management, CGI Business Consulting

IA agentique : au-delà de l'enjeu d'adoption, penser la collaboration humain-agent

Avec l'IA agentique, l'enjeu de l'accompagnement au changement n'est plus seulement d'apprendre à utiliser un outil, mais d'apprendre à travailler avec un agent capable de réaliser une partie des tâches et devenant un véritable partenaire de travail. Cela pose un nouveau défi aux sociétés du secteur financier : **créer les conditions d'une collaboration humain-agent efficace, maîtrisée et durable**, en accompagnant la transformation de l'organisation du travail, du management et de la culture d'entreprise.

De l'adoption d'un outil à la collaboration avec un agent

L'IA agentique marque une nouvelle étape dans la transformation du travail. À la différence d'un nouvel outil technologique traditionnel que le collaborateur va utiliser pour exécuter une tâche ou de l'IA générative que le collaborateur va solliciter pour produire ou analyser, l'IA agentique introduit un nouvel acteur, l'agent virtuel, qui va prendre en charge une séquence d'actions, utiliser différents outils et interagir avec son environnement dans les limites qui lui sont données. Il convient donc de revoir le partage des rôles autour du binôme humain-agent. Il ne s'agit pas d'ajouter l'IA aux processus existants mais bien de penser les processus cibles humain + agent.

De nouvelles compétences de collaboration doivent également être développées. Le collaborateur doit en effet apprendre à déléguer une activité à un agent, lui donner le contexte et les bonnes instructions, contrôler son travail et détecter une incohérence, savoir quand lui faire confiance et quand reprendre la main. Il faudra également former le collaborateur à de nouvelles activités à plus forte expertise qu'il pourra prendre en charge grâce au temps libéré par la mise en place de l'agent.

L'IA agentique requiert donc d'accompagner le changement de l'organisation et des pratiques : **pour réussir le changement il faut apprendre à faire travailler ensemble humains et agents IA.**

Du management des collaborateurs au management d'un collectif hybride

L'IA agentique transforme également le rôle du manager : celui-ci ne pilote plus uniquement l'activité réalisée par ses collaborateurs, il doit progressivement organiser un système où certaines activités sont réalisées par l'humain, d'autres assistées par l'IA ou entièrement déléguées à un agent virtuel et contrôlées par l'humain. Son rôle évolue ainsi vers celui d'**un orchestrateur du travail humain-agent,** avec la mise en place d'un mode de supervision hybride et de nouveaux indicateurs d'évaluation de la performance.

L'autonomie des agents exige une nouvelle discipline managériale avec **un enjeu de délégation sans perte de maîtrise.** Le manager est garant de la compréhension du processus et de la clarté des responsabilités, ainsi que de la qualité des résultats et de la capacité de reprise humaine des activités. En environnement réglementé, le manager reste responsable des actes, même

lorsqu'ils sont délégués à des agents virtuels. Il doit s'assurer du contrôle des décisions avec des points de validation humains, de la traçabilité des workflows pour répondre aux exigences du régulateur et du respect des politiques strictes de confidentialité et de sécurité des données.

Le manager doit également rassurer ses équipes face aux craintes de remplacement par les agents IA. Il doit accompagner ses collaborateurs dans l'acquisition de nouvelles compétences et expertises pour trouver leur place dans la nouvelle organisation du travail. Dans cet environnement, le management constitue plus que jamais la « courroie de transmission » de la transformation engendrée par l'IA agentique.

Une nouvelle culture de travail à diffuser

Le développement de l'IA agentique pose un certain nombre de questions touchant à la culture même de l'organisation : la valeur du travail, la responsabilité, la capacité d'adaptation.

Parmi les évolutions anticipées, on peut citer le passage d'une culture de l'exécution à une culture de la délégation et de la supervision, le collaborateur devant définir les règles, le résultat attendu et assurer le contrôle. L'expertise humaine sera davantage fondée sur le jugement, la capacité à détecter des exceptions et prendre des décisions complexes tandis que l'agent IA gérera les tâches du quotidien.

L'IA agentique oblige également à repenser la responsabilité, indissociable de l'autonomie et de la confiance accordée aux agents. Cette confiance devra se construire par l'expérience, en accordant progressivement davantage d'autonomie et en s'appuyant sur des règles formalisées et des mécanismes de contrôle. La visibilité sur les actions réalisées par les agents et les retours d'expérience sur les premières initiatives seront clés pour poser les bases de cette confiance.

L'IA agentique requiert également de renforcer l'agilité de l'organisation afin de pouvoir ajuster les processus au fur et à mesure que les agents virtuels prennent en charge davantage de tâches en autonomie. En conséquence, l'organisation et les collaborateurs devront s'adapter rapidement à l'évolution des activités.

En conclusion, le défi du change management est d'accompagner cette nouvelle organisation du travail, en construisant confiance, maîtrise et autonomie. L'IA agentique suppose de passer d'un accompagnement au changement centré sur



l'adoption à **un accompagnement centré sur la collaboration.** Les institutions financières doivent également renforcer **une culture de changement continu** afin de favoriser l'agilité organisationnelle requise.

Enfin, le change management peut être lui aussi augmenté par l'IA agentique. L'accompagnement au changement peut s'appuyer sur l'IA pour analyser les retours, détecter les difficultés d'appropriation, personnaliser certains contenus ou accélérer la préparation d'actions de change management, permettant d'avoir une approche plus ciblée et plus impactante.

Remerciements

Ce livre blanc est le fruit d'une réflexion menée par l'équipe Finance Innovation, en collaboration avec les équipes de CGI Business Consulting et de CGI en France.

Réalisé en totale indépendance et intégralement autofinancé, ce livre blanc – ses hypothèses comme ses conclusions – reflète uniquement les convictions de CGI et CGI Business Consulting et engage leur seule responsabilité.

Les travaux ont été menés avec l'appui de contributeurs CGI :

Stéphane Houin

Barbara Rallu

Gilles Cymbalista

Stéphane Marechal

Kinda Nejem

Mikael Mandaglio

Anna Ray

Mourad Aouini

Ines Bouzid

Stéphanie Buet

Victoria Vandenberghe

Charlène Mansier

Les témoignages présentés dans ce livre blanc sont issus d'interviews réalisées par CGI avec des membres du Pôle Finance Innovation, que nous remercions pour le temps qu'ils nous ont accordé :

Patrick Pansier

Responsable Data, Digital & Innovation, LBP AM

Florence Picard

Membre agrégé de l'Institut des Actuaires

Guy-Matthieu Verwaerde

CEO et Cofondateur, StudyAssur

Ossama Benbouidda

Responsable processus et organisation, Caisse des Dépôts

Tang Loaec

Cofondateur, Deepika



Annexes

Lexique minimal

Agent IA

Système capable de poursuivre un objectif, planifier des étapes, utiliser des outils et produire ou déclencher des actions dans un périmètre défini.

AgentOps

Désigne l'ensemble des pratiques et outillages visant à gérer le cycle de vie complet des agents en production, incluant leur déploiement, supervision, monitoring, versioning, sécurité, gestion des incidents et amélioration continue. Cette approche englobe toutes les étapes nécessaires pour assurer un fonctionnement optimal et sécurisé des agents tout au long de leur utilisation.

Human-in-the-loop

Mode d'organisation dans lequel un humain intervient pour valider, superviser, corriger, arbitrer ou contrôler les sorties ou actions de l'agent.

Contexte

Ensemble des données, documents, règles, historiques, outils et instructions auxquels l'agent a accès pour agir.

Autonomie encadrée

Capacité d'un agent à agir dans un périmètre limité, surveillé, réversible et auditable.

Ligne rouge

Usage, action ou décision que l'organisation interdit à l'agent, quel que soit son niveau de performance.

Context inflation (Surcharge contextuelle)

Augmentation excessive de la taille de la fenêtre de contexte qui dégrade la précision du modèle, augmente les hallucinations et fait exploser les coûts en tokens.

MCP (Model Context Protocol)

Standard ouvert permettant de connecter de manière sécurisée et uniforme des modèles d'IA à des sources de données locales ou distantes et à des outils tiers.

Sandboxing (Isolation d'exécution)

Environnement virtuel hermétique dans lequel l'agent exécute du code ou des actions sans pouvoir altérer le reste du système d'information.

Télémétrie

Collecte continue et automatique des données techniques (requêtes, appels d'API, temps de réponse, tokens) pour assurer la traçabilité complète de l'activité de l'agent.

Modèle monolithique vs Micro-agents

Opposition entre un agent unique exécutant l'ensemble des tâches et une architecture multi-agent distribuée, où plusieurs micro-agents collaborent de manière ciblée pour résoudre un besoin complexe.

Références complémentaires utilisées

[E1] European Banking Authority, AI Act implications for the EU banking and payments sector, 21/11/2025.

URL : eba.europa.eu/sites/default/files/2025-11/d8b999ce-a1d9-4964-9606-971bbc2aaf89/AI%20Act%20implications%20for%20the%20EU%20banking%20sector.pdf

[E2] European Banking Authority, Rising application of AI in EU banking and payments sector, 2025.

URL : eba.europa.eu/sites/default/files/2025-09/146b3558-d026-47bf-a872-f05e93ed30d2/Rising%20application%20of%20AI%20in%20EU%20banking%20and%20payments%20sector.pdf

[E3] European Insurance and Occupational Pensions Authority, Opinion on Artificial Intelligence governance and risk management, 2025.

URL : www.eiopa.europa.eu/publications/opinion-artificial-intelligence-governance-and-risk-management_en

[E4] ACPR - Banque de France, Gouvernance des algorithmes d'intelligence artificielle dans le secteur financier, mise à jour 2025.

URL : acpr.banque-france.fr/fr/publications-et-statistiques/publications/gouvernance-des-algorithmes-dintelligence-artificielle-dans-le-secteur-financier

[E5] ESMA, Digital Operational Resilience Act (DORA), page de référence.

URL : www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora

[E6] NIST, Artificial Intelligence Risk Management Framework Generative Artificial Intelligence Profile, NIST AI 600-1, 2024.

URL : www.nist.gov/publications/artificial-intelligence-risk-management-framework-generative-artificial-intelligence

[E7] ISO/IEC 42001:2023, Information technology - Artificial intelligence - Management system.

URL : www.iso.org/standard/42001

[E8] CNIL, Les fiches pratiques IA.

URL : www.cnil.fr/fr/les-fiches-pratiques-ia

[E9] OWASP Top 10 for Agentic Applications for 2026, 9/12/2025.

URL : genai.owasp.org/2025/12/09/owasp-top-10-for-agentic-applications-the-benchmark-for-agentic-security-in-the-age-of-autonomous-ai/



À propos de CGI

Insights you can act on

Fondée en 1976, CGI figure parmi les plus importantes entreprises de services-conseils en technologie de l'information (TI) et en management au monde. Nous sommes guidés par les faits et axés sur les résultats afin d'accélérer le rendement de vos investissements. À partir de centaines de bureaux à l'échelle mondiale, nous offrons des services-conseils complets, adaptables et durables en TI et en management. Ces services s'appuient sur des analyses mondiales et sont mis en œuvre à l'échelle locale.

cgi.com

À propos de Finance Innovation

Créé en 2007 par le ministère de l'Économie et la Région Île-de-France, avec le soutien de Paris Europlace, Finance Innovation est le pôle de compétitivité dédié à l'innovation financière. Acteur d'intérêt général et tiers de confiance au service de son écosystème, il constitue la plateforme stratégique de référence au croisement des institutions financières, des fintechs et des pouvoirs publics.

Sa mission : accélérer la transformation numérique et durable du secteur financier en fédérant l'ensemble des acteurs, institutions financières, grandes entreprises, fintechs, regtechs, insurtechs, investisseurs, pour renforcer la compétitivité de l'économie française, en France et à l'international, et soutenir la création d'emplois.

finance-innovation.org